ORDER

6110.11C

MAINTENANCE OF THE TRAFFIC MANAGEMENT SYSTEM (TMS)

March 5, 1999
Version 1.02

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

Distribution: Selected Airway Facilities Field and Regional Offices; ZAF-600

Initiated By: AOS-330

RECORD OF CHANGES

DIRECTIVE NO. 6110.11C

VERSION ID	DATE	VERSION MODIFICATIONS
1.0	Feb - 99	World Wide Web Baseline
1.01	02/04/99	Chapter 7 TMU Corrective Verification Maintenance Updates Changes to Verification wording (Document Wide). Updates to Document Diagrams
1.02	03/05/99	Partial incorporation of initial Version 1.01 comments Updates to Chapter 6 TMU Routine Verification Maintenance

1 FOREWORD

1.1 PURPOSE.

This Order provides guidance and prescribes technical standards, tolerances, and procedures applicable to the maintenance and inspection of the Traffic Management System (TMS). It also provides information on special methods and techniques that enable maintenance personnel to achieve optimum performance from the equipment. This information augments information available in instruction books and other handbooks, such as the *Enhanced Traffic Management System (ETMS) System Administration Manual*, and complements the latest edition of Order 6000.15, *General Maintenance Handbook for Airway Facilities (AF)*.

1.2 DISTRIBUTION.

This directive is distributed to selected offices and services within Washington headquarters, the William J. Hughes Technical Center, the Mike Monroney Aeronautical Center, the regional AF divisions, and AF field offices with TMS equipment.

1.3 CANCELLATION.

This Order, 6110.11C, is for the Open Systems version of the Traffic Flow Management Infrastructure (TFMI). Order 6110.11B, *Maintenance of the TMS*, will continue to be applicable for those Apollo based sites that have not yet been upgraded to the Open System configuration. When the new Open System upgrade is deployed at a TMU site, this Order, 6110.11C, will then cancel 6110.11B for the old Apollo TMU site and this Order, 6110.11C, will be applicable to the new Open System TMU site.

1.4 MAINTENANCE AND MODIFICATION POLICY.

a. the maintenance technician shall consult and use Order 6000.15, this Order, and the applicable equipment instruction books in all duties and activities for the maintenance of the TMS. These documents shall be considered collectively as the single official source of maintenance policy and direction authorized by Operational Support (AOS). References in this Order, entitled Routine Maintenance and Verification, indicate whether this Order and/or the equipment instruction book shall be consulted.

b. The latest edition of Order 6032.1, *Modifications to Ground Facilities, Systems and Equipment in the National Airspace System (NAS)*, contains comprehensive policy and direction concerning the development, authorization, implementation, and recording of modifications to facilities, systems, and equipment in commissioned status. It supersedes all instructions published in earlier editions of maintenance technical handbooks and related directives.

c. Modifications to equipment listed in *NAS-MD-001, NAS Configuration Management (CM) Document*, as baselined under configuration management, shall be performed according to the latest edition of Order 1800.8, NAS Configuration Management.

1.5 FORMS.

In addition to the forms required by the latest edition of Order 6000.15, FAA Form 6000-8, and *Technical Performance Record (TPR)*, will be maintained for each TMS facility. These forms are available from the

FAA Logistics Center (FAALC) in units of pads, with 50 sheets per pad.

1.6 RECOMMENDATIONS FOR CHANGES.

This Order is under CM control as defined in Order 1800.8 and *NAS-MD-001*. Any changes to the baseline documents or requests for deviation from national standards shall be processed through the NAS Change Proposal (NCP) process. Refer to FAA Form 1800-2, *NAS Change Proposal.*

George W. Terrell
Program Director for Operational Support

TABLE OF CONTENTS

1 FOREWORD V

1.1 PURPOSE V
1.2 DISTRIBUTION V
1.3 CANCELLATION V
1.4 MAINTENANCE AND MODIFICATION POLICY. V
1.5 FORMS V
1.6 RECOMMENDATIONS FOR CHANGES. VI

2 GENERAL INFORMATION AND REQUIREMENTS 1

2.1 OBJECTIVE. 1
2.2 SAFETY. 1
2.3 COORDINATION. 1
2.4 CERTIFICATION AND VERIFICATION. 1
2.5 AIRCRAFT ACCIDENT. 2
2.6 FLIGHT INSPECTION. 2
2.7 TECHNICAL EVALUATION. 2
2.8 VERIFICATION MAINTENANCE 3
2.9 ROUTINE MAINTENANCE. 3
2.10 CORRECTIVE MAINTENANCE 3
2.11 TEST EQUIPMENT AND TOOLS FOR PERIODIC MAINTENANCE. 3
2.12 REFERENCES 3

3 ETMS DESCRIPTION (GENERAL) 5

3.1 NATIONAL AIRSPACE SYSTEM OVERVIEW 5
3.2 ETMS CONCEPT OF OPERATIONS 7
3.3 ETMS SYSTEM OVERVIEW (WAN NETWORK) 10
3.4 ETMS FUNCTIONALITY 12
3.4.1 HUB FUNCTIONALITY 14
3.4.2 TMU REMOTE FUNCTIONALITY 16
3.4.3 INTEGRATED SYSTEM CONCEPT 19
3.5 ETMS TRANSITION CONCEPT 19

4 TMU EQUIPMENT CONFIGURATIONS (DETAILED) 21

4.1 TMU ARTCCS AND CERAPS CONFIGURATIONS 21
4.2 TMU TRACON, TOWER, AND REGIONAL OFFICE CONFIGURATIONS 23
4.3 TMU SYSTEM COMPONENTS 23
4.4 ETMS AUXILIARY EQUIPMENT 26

5 ETMS TMU VERIFICATION MAINTENANCE CONCEPT 32

5.1 THE CONCEPT 32
5.2 TYPES OF VERIFICATION. 32
5.2.1 SERVICE LEVEL. 32
5.2.2 SYSTEM LEVEL. 32
5.3 VERIFICATION RESPONSIBILITY. 32

6 TMU ROUTINE VERIFICATION MAINTENANCE 34

6.1 GENERAL OVERVIEW. 34
6.2 PERIODIC PERFORMANCE CHECKS 37
6.2.1 OVERVIEW 37
6.2.1.1 DAILY. 37
6.2.1.2 WEEKLY 38
6.2.1.3 MONTHLY 38
6.2.1.4 BIMONTHLY. (every 2 months) 38
6.2.1.5 QUARTERLY. 39
6.2.1.6 SEMIANNUALLY – (RESERVED) 39
6.2.1.7 ANNUALLY – (RESERVED). 39
6.2.2 DETAILED PROCEDURES 40
6.2.2.1 TMU FILE SERVER SWITCHOVER CHECK (WKSTN01 TO WKSTN02) 40
6.2.2.2 TMU FILE SERVER SWITCHOVER CHECK (WKSTN02 TO WKSTN01). 41
6.2.2.3 HP UX DIAGNOSTIC CHECK. 41
6.2.2.4 TMU TO TMCCC COMMUNICATIONS CHECK 41
6.2.2.5 TMU TO TMCCC TO TMU COMMUNICATIONS CHECK 42
6.2.2.6 LAN ETHERNET ping CHECK. 42
6.2.2.7 LAN ETHERNET netstat CHECK 42
6.2.2.8 TMU SYSTEM ERROR LOGS CHECK 43
6.2.2.9 CISCO 1601 ROUTER OPERABILITY CHECK 43
6.2.2.10 LIST VOLUME FREE SPACE. 43
6.2.2.11 CISCO 1601 ROUTER ERROR LOG CHECK 44
6.2.2.12 STANDBY CISCO 1601 ROUTER RE-INITIALIZATION 44
6.2.2.13 UPS AVAILABILITY TEST. 44
6.2.2.14 ATCSCC COMMUNICATIONS CHECK 45
6.2.2.15 TMU FILE SERVER TO HOST/ARTS COMMUNICATIONS CHECK 45
6.2.2.16 SPARE CISCO ROUTER SWITCHOVER CHECK. 46
6.2.2.17 SPARE CISCO ROUTER A/B SWITCHOVER CHECK. 46
6.3 NON-PERIODIC PERFORMANCE CHECKS 46
6.3.1 OVERVIEW 47
6.3.2 NON-PERIODIC PERFORMANCE CHECKS SCHEDULE 47
6.3.3 NON-PERIODIC PERFORMANCE CHECKS DETAILED PROCEDURES 49
6.3.3.1 PERFORM SYSTEM SETUP PROCEDURES 49
6.3.3.2 CLEAN TAPE TRANSPORT 49
6.3.3.3 REMOVE OBSOLETE 56-DAY UPDATE FILES 49
6.3.3.4 CLEAN ALL CPU TOWER AIR INTAKE AND EXHAUST VENTS. 49
6.3.3.5 ADJUST MONITOR CONTROLS 49
6.3.3.6 CLEAN ALL WORKSTATION MONITOR VIEWING PANELS. 50
6.3.3.7 CLEAN ALL COMPUTER CABINET, MONITOR CABINET, KEYBOARD< TRACKBALL, AND PRINTER HOUSINGS 50
6.3.3.8 HP TMCCC DATA REDUCTION. 50

7 TMU CORRECTIVE VERIFICATION MAINTENANCE 51

7.1 CORRECTIVE MAINTENANCE VERIFICATION PHILOSOPHY 51
7.2 TMU OPERABILITY ASSESSMENT 51
7.3 TMU CORRECTIVE MAINTENANCE APPROACH 60
7.3.1 GENERAL CORRECTIVE MAINTENANCE APPROACH 60
7.3.2 SOFTWARE FAILURES (GENERAL) 60
7.3.3 HARDWARE FAILURES (GENERAL) 60
7.3.4 RESTORATION (GENERAL) 61
7.3.5 CORRECTIVE MAINTENANCE LOG AND THE LOGGING OF OPERATIONAL INCIDENTS 61
7.3.6 MAJOR TMU COMPONENTS FAULT DETECTION, ISOLATION, AND RESTORATION 61
7.3.6.1 Wide Area Network (WAN) Phone Lines 61
7.3.6.1.1 Phone Lines Fault Detection and Isolation 62
7.3.6.1.2 Phone Lines Restoration 62
7.3.6.2 TMU Local WAN Router 62
7.3.6.2.1 TMU Router Fault Detection and Isolation 62
7.3.6.2.2 TMU Router Restoration 63
7.3.6.3 TMU LAN Communications Hub 63
7.3.6.3.1 TMU Hub Fault Detection and Isolation 63
7.3.6.3.2 TMU Hub Replacement 64
7.3.6.4 Local Area Network (LAN) Hub Communication Interfaces 64
7.3.6.4.1 LAN Interconnection Fault Detection and Isolation 64
7.3.6.4.2 LAN Restoration 64
7.3.6.5 File Server 64
7.3.6.5.1 File Server Fault Detection and Isolation 65
7.3.6.5.2 File Server Restoration 65
7.3.6.6 Workstation 66
7.3.6.6.1 Workstation Fault Detection and Isolation 66
7.3.6.6.2 Workstation Restoration 68
7.3.6.7 Monitor 68
7.3.6.7.1 Monitor Fault Detection and Isolation 68
7.3.6.7.2 Monitor Restoration 68
7.3.6.8 Keyboard 68
7.3.6.8.1 Keyboard Fault Detection and Isolation 68
7.3.6.8.2 Keyboard Restoration 69
7.3.6.9 Trackball 69
7.3.6.9.1 Fault Detection and Isolation 69
7.3.6.9.2 Trackball Restoration 69
7.3.6.10 Tape Station 70
7.3.6.10.1 Tape Device Fault Detection and Isolation 70
7.3.6.10.2 Tape Station Restoration 71
7.3.6.11 Printer 71
7.3.6.11.1 Printer Fault Detection and Isolation 71
7.3.6.11.2 Printer Replacement 71
7.3.6.12 File Server to NAS ATC Computer Interface 72
7.3.6.12.1 NAS Interface Fault Detection and Isolation 72
7.3.6.12.2 NAS Interface Restoration 73
7.3.6.13 Tower LAN Interface 73
7.3.6.13.1 Control Tower Fault Detection and Isolation 73
7.3.6.13.2 Control Tower Restoration 73
7.3.6.14 UPS 73

7.3.6.14.1 UPS Fault Detection and Isolation 74
7.3.6.14.2 UPS Restoration 76
7.3.6.15 Surge Supressors 76
7.3.6.16 A/B Switches 76
7.3.6.17 Repeaters 76
7.3.6.18 Cables and Connectors 76

8 ABBREVIATIONS AND ACRONYMS 77

APPENDIX A. CAPABILITIES VERIFICATION REQUIREMENTS 83

LIST OF FIGURES

Figure 3-1 ETMS Concept of Operations 8
Figure 3-2 ETMS Wide Area Communications Network 11
Figure 3-3 ETMS Apollo-to-Open Systems Transition Diagram 13
Figure 3-4 ETMS Functional Diagram 15
Figure 4-1 Typical ARTCC Open Systems Configuration 22
Figure 4-2 Typical TRACON (With Tower) TMU Open Systems Configuration 24
Figure 4-3 Regional Office Configuration 25
Figure 4-4 File server Configuration 27
Figure 4-5. 24-Port Hub 28
Figure 4-6. Cisco 1601 Router 29
Figure 4-7. APC Smart UPS 30
Figure 6-1 Technical Performance Record (Page 1 of 2) 35
Figure 6-2 Technical Performance Record (Page 2 of 2) 36
Figure 7-1 Operability Assessment Tools 53

LIST OF TABLES

Table 5-1 TMU Open Systems Maintenance Concept 33

Table 6-1 Periodic Performance Checks Schedule 37

Table 6-2 Non-periodic Performance Checks 48

Table 7-1 Operability Assessment Tools Functionality 54

Table A-0-1. TSD Capabilities Verification Requirements 83

2 GENERAL INFORMATION AND REQUIREMENTS

2.1 OBJECTIVE.

This Order provides the necessary guidance for the proper maintenance of the TMS. It should be used in conjunction with information available in instruction books and other handbooks, such as the *ETMS System Administration Manual.*

2.2 SAFETY.

Personnel shall observe all pertinent safety precautions when performing duties on the equipment. For guidance, refer to the latest edition of Order 6000.15.

2.3 COORDINATION.

a. Maximum availability is of prime importance to the users of AF systems, services, and equipment. Maintenance should therefore be accomplished, to the extent practicable, on the offline (backup) operating equipment. When necessary to perform maintenance on the online operating equipment, it shall be coordinated with the appropriate personnel, precluding unanticipated shutdowns. In most cases, one can perform maintenance without interrupting operations by using ETMS backup capabilities such as file server switchover.

b. AF personnel shall be familiar with the role of the TMS in the NAS so that facility shutdowns can be coordinated with the proper agency and non-agency personnel. Specifically, AF personnel shall thoroughly coordinate, in advance, with the Air Traffic Operations (ATO) personnel any maintenance activity that may adversely affect the use of a commissioned facility. Furthermore, AF personnel must be familiar with ATO procedures to ensure that notification is made sufficiently early to allow ATO personnel to take appropriate action. It is expected that ATO personnel recognize the need for releasing equipment at the time scheduled for maintenance and cooperate in the furtherance of practices that assure continuous and reliable operation. See the latest edition of Order 6000.15 for additional guidance.

c. When a shutdown is successfully scheduled, Air Traffic (AT) personnel shall initiate an Air Traffic Advisory announcing the shutdown. See the latest edition of *Order 6030.5, Service Availability of Commissioned Facilities of the National Airspace System,* for details on this procedure.

d. AF personnel are responsible for keeping ATO personnel advised of the operational status of all systems, subsystems, facilities and equipment. When unscheduled interruptions occur, prompt notification shall be made to cognizant ATO personnel. They shall be advised immediately when equipment fails, service is restored, the established tolerances are exceeded, or the established tolerances are expected to be exceeded so that the ATO can issue Air Traffic Advisory messages, reroute air traffic, and/or take other necessary action. This activity is especially important where standby or spare equipment is not immediately available.

2.4 CERTIFICATION AND VERIFICATION.

a. References. Refer to the latest edition of Order 6000.15 for guidance on the certification of services and systems. Refer to this Order for specific requirements applicable to the

verification of the TMS automation services, systems, and equipment; the associated verification parameters; the nominal and maximum verification intervals; the identity of recommended personnel responsible for verification; the prescribed verification statement to be entered in the Traffic Management Unit (TMU) Log. Appendix A will be elaborated in future versions of this Order.

b. Required Certification.
Certification is not required for the following services and systems:

1) Traffic Management Service
2) Traffic Management System (TMS)

c. Required Verification.

While formal certification is not required for the Traffic Management Service and the System, every effort should be made to verify that the Traffic Management Service and the System are performing acceptably. This verification takes the form of ensuring correct system responses to Human-Computer Interface (HCI) Commands, online operability checks, maintenance diagnostics, correctly performed routine maintenance, appropriate coordination with hot line(s) for those observed phenomena that may not be fully understood, proper investigation and reporting of known problems through formal procedures, and corrective maintenance that returns a fully operational system to online status.

2.5 AIRCRAFT ACCIDENT.

a. General. AF personnel must support the procedures established in the latest edition of Order 8020.11, Aircraft Accidents and Incidents-Notification, Investigation, and Reporting.

b. Preliminary Notice. When an accident occurs, ATO personnel identify those facilities potentially involved in the accident and notify the appropriate AF personnel. AF personnel must then provide ATO with the information they require to report the operational status of the facility on FAA Form 8020-9, Aircraft Accident/Incident Preliminary Notice. Furthermore, any system adjustments that alter the established value of parameters that may be checked in a technical facility evaluation should be postponed until after the associated measurements or flight checks have been performed, unless otherwise directed.

c. AF Accident Investigation. After the ATO releases the accident notification message, the System Management Office Manager initiates a technical facility evaluation. In addition, the Regional AF Division designates a Regional AF Accident Representative as a coordinator of the AF contribution to the accident investigation and as a liaison with the FAA Investigator in charge. Refer to Order 8020.11 for the details of the organization of and the procedures for the investigation and reporting of a TMS-related aircraft accident or incident.

d. Records. It is imperative that all records always be kept current, concise, and accurate. All station records, such as Facility Maintenance Logs and Technical Performance Records, are official documents. As such, they are used in investigations of aircraft accidents and other situations when the facility operation is questioned.

2.6 FLIGHT INSPECTION.

The TMS receives no direct sensor inputs. Thus, all TMS inputs undergo required flight inspection under other system procedures; no TMS flight inspection is required.

2.7 TECHNICAL EVALUATION.

Facility inspections are among the most effective management controls for ensuring

the required level of maintenance work and equipment and system performance. See the latest edition of Order 6000.15 for general guidance on inspections and the latest edition of Order 6040.6, *Airways Facilities Technical Evaluation Program* (RIS:AF 6040-8), for details on the intervals and requirements for formal inspections.

The Traffic Management Central Computer Complex (TMCCC), located at Volpe, is a non-FAA facility staffed by non-FAA personnel. While FAA Orders may not directly apply to the TMCCC, the general applicability of their content does.

2.8 VERIFICATION MAINTENANCE

Chapter 5 of this Order establishes the Verification Maintenance philosophy for the TMS TMU system components. Routine Maintenance and Corrective Maintenance are the two primary Verification Maintenance categories.

2.9 ROUTINE MAINTENANCE.

Chapter 6 of this Order establishes the tasks and schedules required for the routine maintenance of the TMS TMU system components. These tasks, as scheduled, are the minimum required for the TMS to meet minimum performance standards.

2.10 CORRECTIVE MAINTENANCE

Chapter 7 of this Order establishes the methodology and procedures for TMU corrective maintenance.

2.11 TEST EQUIPMENT AND TOOLS FOR PERIODIC MAINTENANCE.

The test equipment required for performing routine maintenance of the TMS are managed by the latest edition of Order 6200.4, *Test Equipment Management Handbook.* Tools and supplies are specified and managed by the latest edition of Order 4630.2, *Standard Allowance of Supplies and Working Equipment for National Airspace System Facilities.* No specific test equipment is required.

2.12 REFERENCES

a. Instruction Books. The instruction books applicable to the TMS equipment are listed below.

1) The HP/UX System Administration Handbook and Toolkit
2) HP Model C160/C180/C200/C240 /360 Owner's Guide A4200-90033
3) HP A4576 21-inch Color Monitor User's Guide
4) HP Hardware Installation Card C Class A4200-90012
5) HP IPR/Diagnostic Media User's Guide PA-RISC Computer Systems B6191-90007
6) HP Recovery Media User's Guide PA-RISC Computer Systems B3782-90210
7) HP Common Desktop Environment (CDE) 1.0 User's Guide B1171-90101
8) HP CDE Getting Started Guide B1171-90104
9) HP CDE Quick Reference Card A Tour of CDE
10) HP Advanced User's and System Administrator's Guide B1171-90102
11) HP Tape Desktop & Rack-Ready Drives Users Manual A1658-90703
12) HP FAST CD-ROM Disc Drive User's Guide A1449-90602
13) HP 2-GB, 4-GB & 9-GB Ultra SE Disk Drive User Notes

14) Cisco 1600 Series Hardware installation Guide 78-3086-02
15) Cisco 1600 Series Software installation Guide 78-4486-01
16) HP Deskjet 1600 CM Color Printer
17) APC Certificate of Guarantee 990-0501 Rev 1/2-92
18) *User's Manual - Smart UPS* 990-2001-A8/10-93 990-7016-A 990-2008
19) FAA ETMS Tech Notes
20) FAA ETMS Site Program Bulletins
21) ETMS System Design Documents (SDD) Volumes 1 and 2
22) HP System Administration Manager (SAM) Manual (commercial documentation)
23) HP Support Tool Manager (STM) Manual (commercial documentation)

b. Other Equipment Documentation. The TMS uses equipment whose maintenance is not covered in this Order. See the latest edition of Order 6170.10, Maintenance of Data Multiplexing Network Equipment, for modem maintenance.

c. ETMS Site Program Bulletins. A set of current ETMS Site Program Bulletins is also used to provide on-site AF personnel guidance on specific matters pertaining to the TMS maintenance program

d. System Verification. System verification information is available in the following documents.

1) *Operational Requirements: System Description of the Traffic Management System, Phase 2 Enhancements* FAA-OR-2783C

2) *Enhanced Traffic Management System (ETMS) Functional Description* VNTSC-DTS56-TMS-004

3) *Traffic Situation Display (TSD) Tutorial,* VNTSC-DTS56-TMS-005

4) *TSD Reference Manual* VNTSC-DTS56-TMS-004

5) *TSD Quick Reference Guide TSC-DTS56-TMS-006*

6) *Traffic Management System FAA Order 7210.47*

7) *Traffic Management System Automation Enhancements Master Test Plan*

8) *Project Implementation Plan for the Traffic Management System (TMS) FAA Order 6110.12A*

9) *TMS System Fault Isolation Student Guide NYMA* CDRL 055

10) *ETMS Field Operations Manual, Version 6.X* VNTSC-DT556-TMS-001

3 ETMS DESCRIPTION (GENERAL)

3.1 National Airspace System Overview

The ETMS is one of five major computer-based systems that comprise the National Airspace System (NAS).

The other four are the En Route System, Terminal Radar Approach Controls (TRACONs), Oceanic (DOTS), and the Flight Service System (FSS). In addition to these five major system components, NAS includes a vast array of Navigation Aids (NAVAIDs), radar equipment including transponders, Weather systems, digital and analog voice and message communication systems including radio, an elaborate system of airways, airports with control towers, documentation, and personnel. NAS is a system of systems with a high degree of interoperability and online message interface between the major system components.

The En Route System includes 21 Air Route Traffic Control Centers (ARTCCs). Twenty are located in the Continental United States (CONUS) and one is located in Alaska. Each ARTCC includes a large International Business Machines (IBM) main frame Host computer that keeps track of flight plans for the traffic in those sectors comprising the ARTCC. The ARTCC Host computer also receives near real-time live radar reports. These radar reports indicate the position of all airborne traffic detected in the ARTCC airspace. The Host computer processes the ARTCC data and displays sector boundaries and sector traffic on individual displays. Air Traffic Controllers then use this display information to control air traffic in their respective sector(s). As airplanes traverse the airspace boundary between adjacent sectors within an ARTCC and between ARTCCs, a controller handoff occurs.

The current En Route IBM computer systems are being upgraded to modern IBM 390 mainframe computers and the En Route Display Subsystem is being modernized with the Display System Replacement (DSR) project.

TRACON airspace also exists within an ARTCC boundary. Each major city has an associated TRACON airspace and facility. TRACON airspace exists for a radius of approximately 40-50 miles. Each TRACON contains at least one airport. As airport arrival and departure aircraft traverse a sector boundary between a TRACON and an ARTCC, a controller handoff occurs. The ARTCC Host computers also interface online with all the TRACON (ARTS III A) computers that exist within the ARTCC. The ARTCC Host computers act as the central repository for flight plans. Flight plan messages are exchanged between the ARTCC Host IBM computer and the TRACON ARTS III-A computers. The ARTS III-A computers process flight plans and aircraft radar reports and display sector information on the TRACON sector displays. TRACON controllers then use this display information to control TRACON airspace traffic in their respective sectors.

The current FAA STARS project is intended to modernize the TRACON systems.

As an airplane approaches or departs an airport, Air Traffic Controllers in the control tower receive or handoff control of the aircraft from or to the TRACON. Control towers usually contain a display of airport inbound and outbound aircraft, which is driven by the TRACON ARTS III-A computer. Control Tower-based Air Traffic Controllers must allocate runway resources to inbound arrival traffic and outbound departure traffic. Control Tower ATC controllers must prevent aircraft on the ground from running into each other on and off the runway. If insufficient gate capacity exists at the terminal building, control tower personnel may be required to manage the aircraft until they can be parked at the gate.

Fog causes a serious problem with traffic on the ground at airports because pilot visibility is drastically reduced. High resolution Airport Surveillance Radars are used to provide control tower personnel with aircraft position information while the aircraft are on the ground. This radar helps to prevent runway incursion.

Aircraft over the Atlantic and Pacific oceans, unless close to the shore, will not be within radar coverage because the range of a long-range radar is normally between 200 and 300 miles. Oceanic air traffic is monitored and controlled by means of the DOTS system. A DOTS system is located in California for the Pacific Ocean and in New York for the Atlantic Ocean. Pilots flying Instrument Flight Rules (IFR) over the ocean will periodically radio their position and corresponding time. This analog or digital radio message will be picked up by long-range ARINC radio receivers. The data messages from these radio receivers is then networked into the Oceanic Control Centers where the DOTS equipment is located. Controllers situated in front of the Oceanic displays then effect the control of oceanic airspace traffic.

Sixty-four automated Flight Service Stations are situated around the CONUS and additional Flight Service Station units are situated in Alaska, Hawaii, and Puerto Rico. Many Flight Service Stations that have not been automated also exist. Flight Service stations do not control air traffic; however, they do provide weather briefings to pilots as part of a pilot's preflight preparation. They also provide weather briefings to pilots while the pilot is airborne, should the pilot request the Flight Service to do so. Flight Service stations provide an important NAS information service to Visual Flight Rule (VFR) pilots. VFR pilots are not normally under ATC. ATC is normally applied only to IFR traffic. Commercial air transport carriers normally fly IFR. General Aviation (GA) may or may not fly IFR. A VFR pilot may request the services of ATC and, if the ATC controller is not too busy, this service may be provided.

The Flight Service System (FSS) consists of a centralized data processing system contained in each ARTCC. Approximately three or four Flight Service Stations, geographically dispersed around the ARTCC Facility, are connected to the central ARTCC Hub. Each Flight Service Station receives up-to-date weather information from individual commercial services. The current FAA OASIS project is intended to modernize the Flight Service System.

Alaska and Hawaii each contain an EARTS, which serve the same function as the 20 continental-based ARTCCs. Alaska also contains an Oceanic system referred to as the Oceanic Control System (OCS).

ETMS consists of a centralized data processing system located at the Volpe National Transportation Center (VNTSC) in Cambridge, Massachusetts. This centralized data processing system is referred to as the ETMS Hub. The ETMS Hub is interfaced through external communications to a Wide-Area Network (WAN). This WAN interfaces some 83 decentralized data processing systems known as TMUs. TMUs are located in each ARTCC, some 35 TRACONs, 2 CERAPs, 8 control towers, 9 Regional Offices, 2 Air Force Bases (AFBs), the FAA Academy, the William J Hughes Technical Center, the FAA Headquarters, and the ATCSCC located in Herndon, Virginia. The TMUs located at the ARTCCs, TRACONs, and Control Towers, CERAPs, and DOTS receive online NAS traffic messages through an online interface to the ATC computers.

3.2 ETMS Concept of Operations

Figure 3-1 illustrates the concept of ETMS operations. The large oval in the top-left area of the diagram represents an En Route ARTCC. The ARTCC contains several radar sets, which send near real-time airborne target positions to the En Route Host data processing system. The illustrated ARTCC also contains two TRACON airspaces. Like the En Route ARTCC, each TRACON contains a building, which houses the computer equipment, from which air traffic is controlled by Air Traffic Controllers using the sector information displays. These displays are referred to as Plan View Displays (PVDs).

Figure 3-1 also illustrates the centralized ETMS data processing Hub, which is situated in the upper-right area of the diagram. The Command Center is situated in the lower-right area of the diagram. The Airline Dispatch Offices are situated in the upper-left area of the diagram, and the TSD Menu is displayed in the center-upper-right area.

The ETMS is principally a scheduling system. ETMS is normally used to schedule air traffic only when problem situations arise. These problem situations may originate because of closed runways that may be closed because of any number of reasons: bad weather from storms and fog, or inoperable navigation or ATC equipment, or just an excess of air traffic demand because of a holiday. ETMS is used when the traffic demand on an airport or airspace sector is larger than the capability of the system to handle the demand. This excess in demand will exceed capacity if some portion of the demand is not rescheduled. An excess of demand over capacity will result in an airborne holding pattern and fuel wastage.

Unless flights are held on the ground (delayed) until such time as they can land on arrival at the destination airport, an airborne holding pattern must be established and managed.

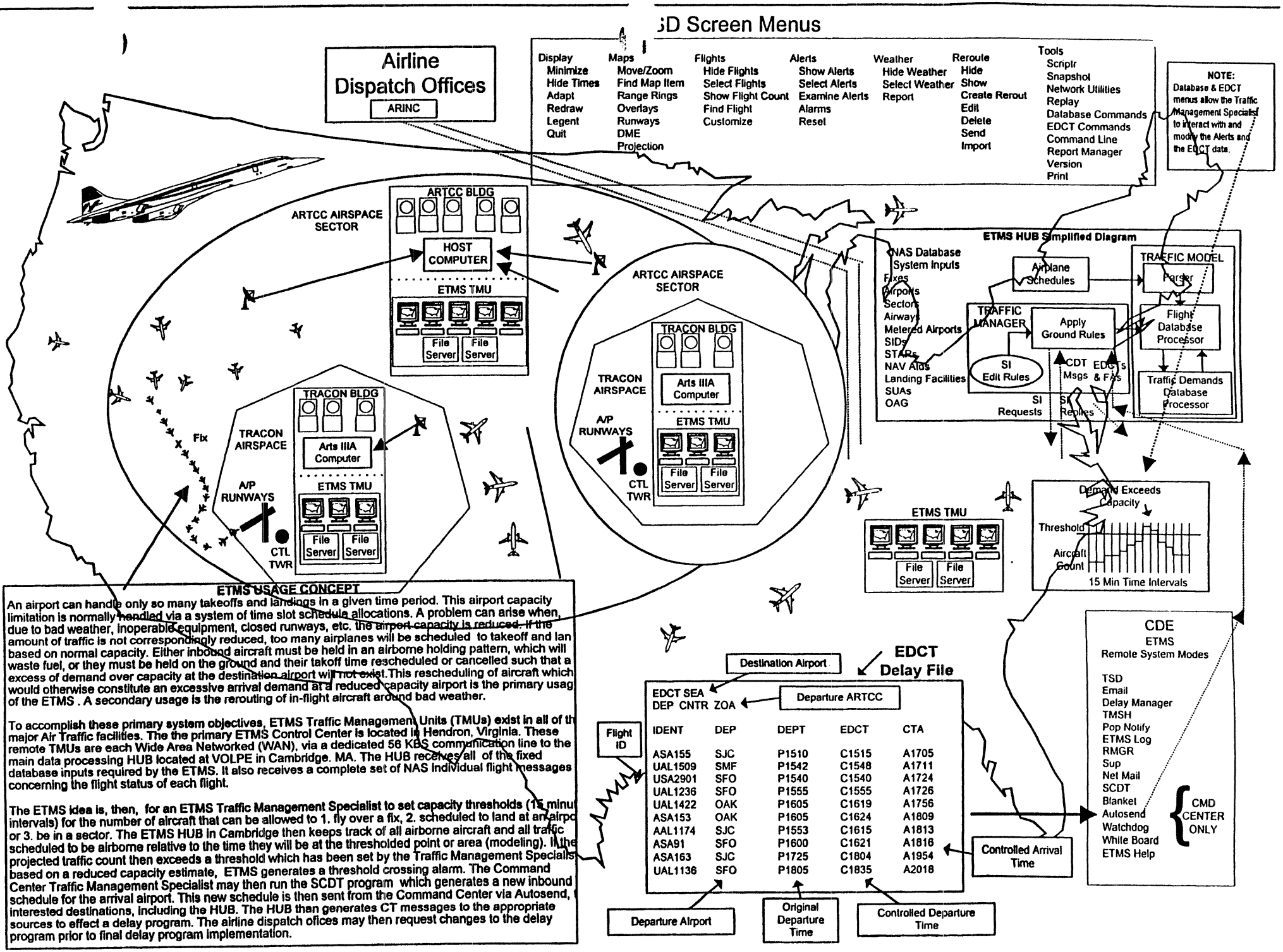


Figure 3-1 ETMS Concept of Operations

Figure 3-1 illustrates this principle with the stream of aircraft flowing toward the airport. If more aircraft are in the flow than the airport runways can handle, the arrivals must be held in a holding pattern until their turn to land. Airborne holding patterns waste fuel and cause an increased load on the Air Traffic Controllers. Rather than hold the excess arrival traffic in a holding pattern, it is more desirable to hold the excessive traffic on the ground until such time as they can fly straight through and land. The main use of ETMS is to derive this new schedule and issue the messages, which delay the takeoff times such that airborne holding patterns are not required. This traffic originates from many different airports at many different times.

The Command Center, depicted in the lower-right area of Figure 3-1, is used to implement what is referred to as a Ground Delay Program. Traffic Management Specialist(s) in the Command Center will first collaborate with airport control, tower personnel to determine what the reduced capacity will be. Weather forecasts and other decision support criteria will be used. Other interested organizational entities such as airlines dispatch personnel will also be included in the collaboration. Agreement will be reached as to what the projected capacity will be. The Command Center will then invoke the SCDT Mode of the CDE, depicted in the lower-right corner of Figure 3-1. SCDT will generate a schedule of all the delayed aircraft in the form of an Estimated Departure Clearance Time (EDCT) Delay file. The contents of this file are key to understanding what the ETMS does and the reader should study the details of the EDCT Delay file as depicted in Figure 3-1. The Command Center Traffic Management Specialist may modify the contents of this file before sending it to the Hub through the CDE Autosend Mode. This interaction can be accomplished by using the TSD Tools Menu EDCT commands. Refer to the upper-left area of the diagram.

The Hub (diagram upper-right) will receive the EDCT File and generate the required messages and distribute them to the affected organizations, including the Airline Dispatch Offices, which participate in the collaborative decision process. The Airlines may then request modifications by submitting SI messages. These SI requests may or may not be honored by the Command Center Traffic Management Specialist. A collaborative type decision process is again entered into by all affected parties and a final Delay Program is then implemented by the Command Center. After the Delay Program is finally implemented, the ETMS Hub sends Control Time (CT) messages to the appropriate ARTCCs. The ARTCC ATC then causes the flights to be delayed for the specified departure (takeoff) time. The airlines affected may also elect to cancel or divert flights.

Figure 3-1 also illustrates the thresholding of demand versus capacity. Refer to the Demand Exceeds Capacity block, which appears in the center on the right side of the diagram. The Traffic Management Specialist in any of the TMUs can use the Database Commands, which appear under the TSD Tools Menu (diagram upper-right) to set a threshold, input general aviation demands, and so on. The projected schedule is normally "sliced" into 15-minute intervals and may cover a period from 1 to 9 hours. The reader should understand the aircraft count includes aircraft presently in air and

aircraft not scheduled for takeoff until some future time. This requirement for future flight projections is one of several reasons the Hub must contain a Traffic Model. The Traffic Model generates the required projections of what the aircraft count for each 15-minute interval will be. After the Traffic Management Specialist has set the threshold, ETMS will generate an alert if the projected demand traffic count exceeds the projected capacity threshold. The alert may cause the Traffic Management Specialist to initiate some type of rescheduling to alleviate the excessive demand versus capacity situation.

In addition to the previously described concept of operation, the ETMS TSD can be used to display airborne flights or any useful subset that may be useful to the Traffic Management Specialist. Weather is also normally depicted on the TSD. This display of weather can aid in defining a reroute program. A reroute affects a modified flight plan to avoid bad weather along the flight route. The pilot then can fly around or over the bad weather, rather than fly through it. Reroutes are managed through the TSD Reroute Menu. This Order also discusses other ETMS features and functionality.

3.3 ETMS System Overview (WAN Network)

Figure 3-2 depicts the ETMS WAN communications layout. The ETMS centralized data processing Hub contains two identical sets of processors. These dual sets are referred to as String A and String B. String A and String B interface with the external communications in such a way that each string carries approximately 50 percent of the TMU sites. Any given TMU is normally connected with either String A or String B, but not to both concurrently.

Each TMU is connected to the Hub through a dedicated 56 KBS line. Some 83 Open Systems remote TMUs will interface in this manner with the Hub. These 56 KBS lines use the TCP/IP communication protocol. The only way one TMU can communicate with another TMU is through the HUB. No direct connections between TMUs exist.

The WAN includes Cisco routers on the Hub end and each TMU end. These routers direct the WAN message traffic to the correct Internet Protocol (IP) address. The Cisco routers are part of the Figure 3-2, External Communications, dual circle area.

WAN message traffic, as depicted in Figure 3-2, is of a variety of types. The ATC facilities forward several different NAS messages the facility uses to control traffic. Each ATC facility forwards its own set of NAS flight messages to the ETMS Hub. The Hub then redistributes the messages received from each ATC facility to the other TMU sites, as required. ATC facilities involved include the ARTCCs, the TRACONs, the Control Towers, the Oceanic, and the CERAPs. The ETMS TMU located in each facility interfaces with the appropriate ATC computer through a special interface module to receive these ATC messages. The TMU then forwards these messages to the Hub, which redistributes them to other TMUs where they are retained in flight databases. Note that these messages are received only from the ATC computers.

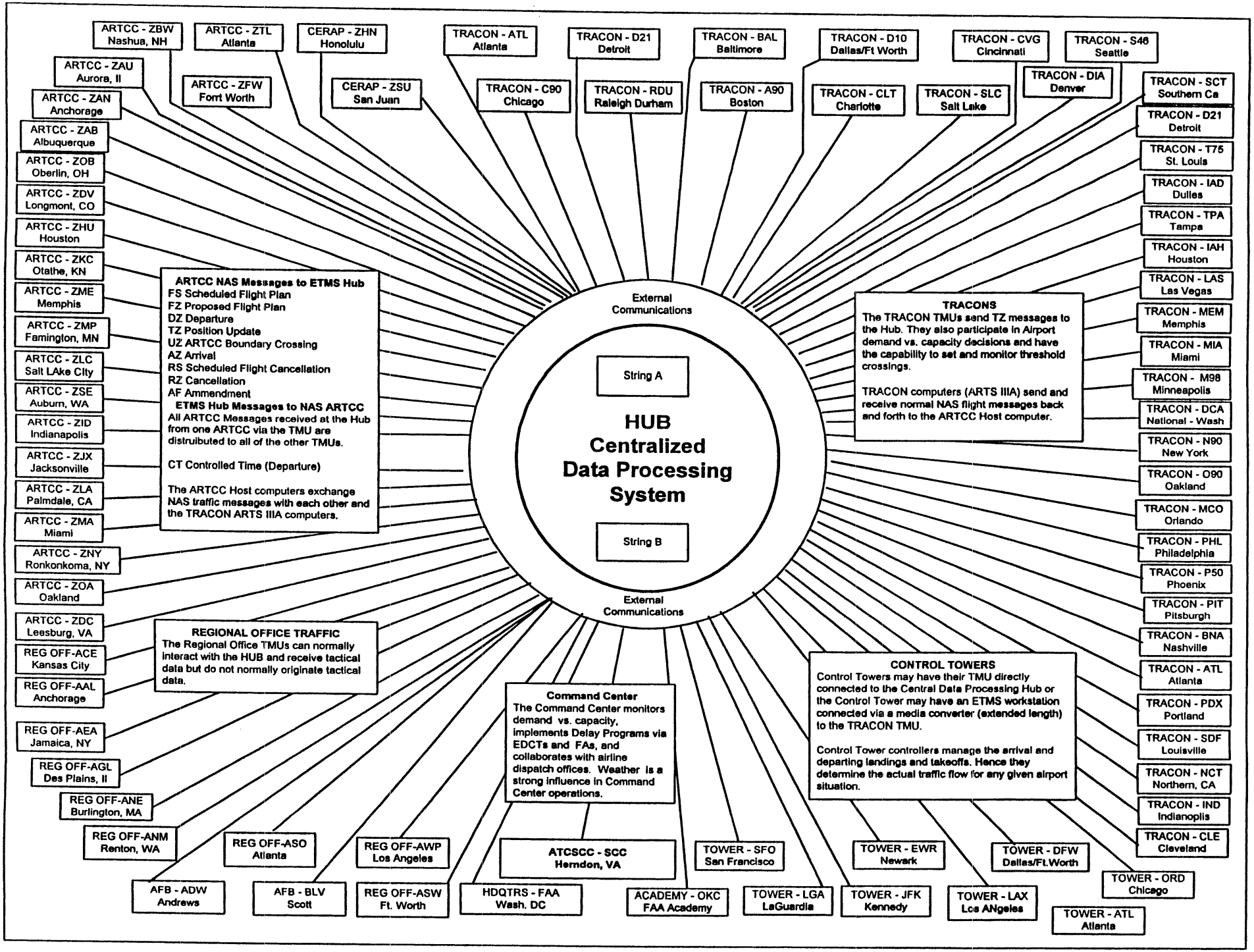


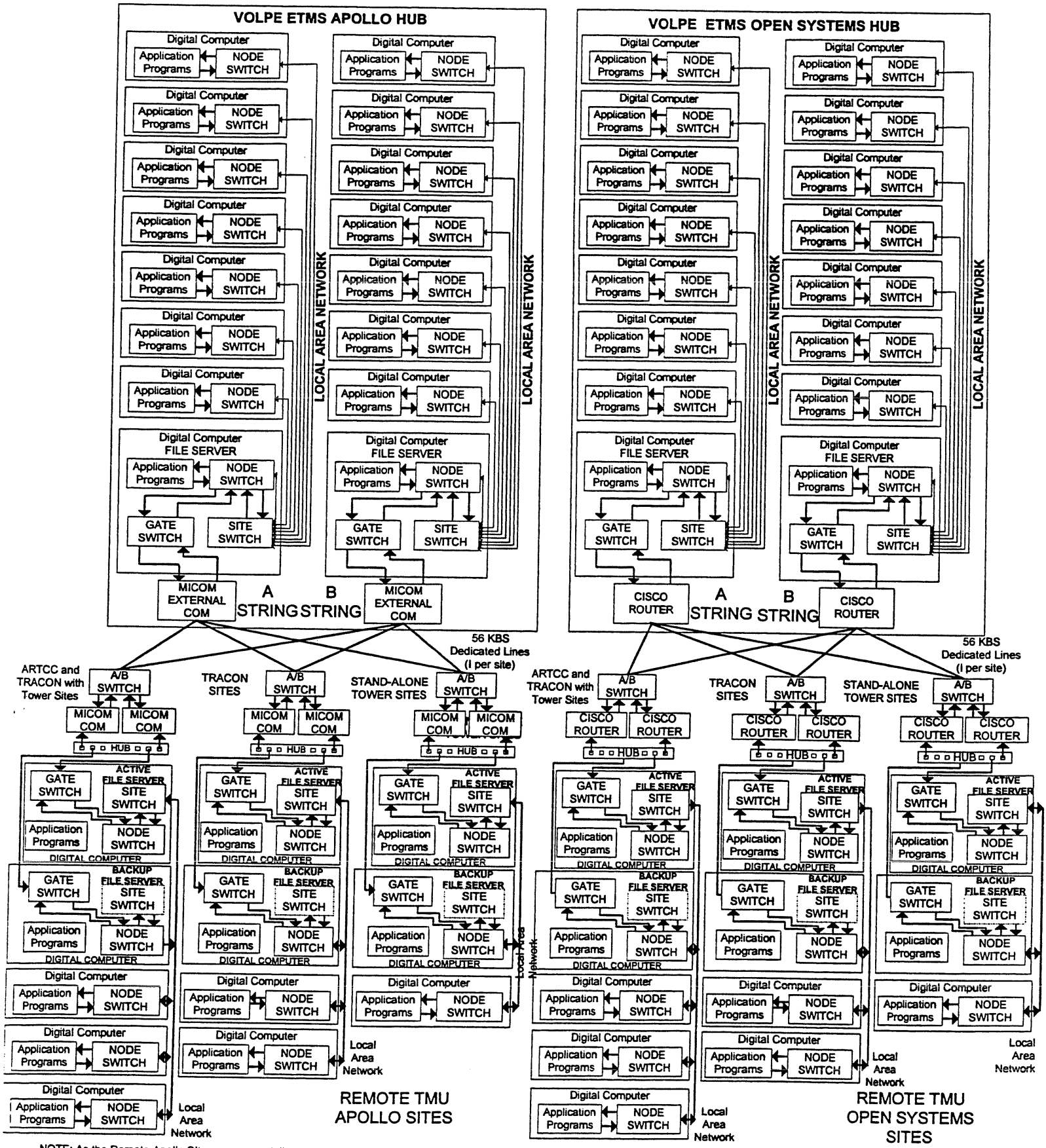
Figure 3-2 ETMS Wide Area Communications Network

In addition to the normal NAS traffic-related messages sent to and distributed by the Hub, each TMU also interfaces with the Hub based on a set of unique ETMS distributed system data requirements. ETMS data from the TMUs to the Volpe Hub include updates to alert status, schedule updates, capacity updates, updates to general aviation demands, traffic management commands, data request messages, messages of a general nature, advisories, e-mail and Net Mail.

ETMS Hub data to the TMUs includes flight data transactions, alert summaries, jet stream, precipitation and lightning weather data, demand data, capacities, general aviation estimates, traffic management data, general messages, e-mail, and Net Mail.

3.4 ETMS Functionality

Figure 3-4 illustrates the ETMS functionality from the overall viewpoint of the combined Hub and TMU. The NAS interfaces are illustrated on the left side of the diagram, the Hub is illustrated at the top of the diagram, the Remote TMU is illustrated at the bottom of the diagram and the right side of the diagram illustrates the concept of processor allocation at both the Hub and the Remote TMU. External communications between the central Hub and the decentralized TMU are also illustrated.



NOTE: As the Remote Apollo Sites are sequentially upgraded to Open Systems Configurations, the Open Systems Configuration is connected to the Open Systems Hub

Figure 3-3 ETMS Apollo-to-Open Systems Transition Diagram

3.4.1 HUB Functionality

The ETMS requires several external database type inputs. Mostly, these are provided through the Hub Auxiliary Support Functions situated in the Hub area on the left side of the diagram. The four principle inputs are the

1. The En Route Adaptation Controlled Environment Systems (ACES) input
2. The National Oceanographic Service (NOS) input
3. The National Flight Data Center (NFDC) input
4. The Official Airline Guide (OAG) input

ACES is generated by the ARTCCs. Twenty-one-input files compose the ACES input. The ACES data consists of fixes, airports, sector definitions, airway definitions, and metered airports. Metered airports are high-density traffic airports. ACES data in the ARTCCs is known as adaptation data, which is used to adapt each of the ARTCCs to its unique geographical and airspace requirements. Each ARTCC updates its ACES adaptation database every 56 days. ETMS receives a copy of each of these 56-day adaptation files.

The NOS data consists of the data used to define the airways. Airways are the predefined navigation routes that IFR flights must fly. Many airways in NAS and the FAA provide an extensive set of airways charts for pilots to use. ETMS uses only the high-altitude IFR routes. The NOS data also includes Standard Instrument Departure (SID) and Standard Arrival Route (STAR) data. Each significant airport has an associated set of standard arrival and departure routes. Airport arrival and departure IFR flights normally use standard SIDs and STARS to affect an orderly traffic flow.

NFDC data includes the Landing Facilities data; NAS NAVAIDs, of which there are many; Airspace fixes, of which there are many; and Special Use Airspace (SUA) definitions. SUAs are the special volumes of airspace allocated for military use. SUAs can be scheduled for usage by the commercial sector when they are not in use by the military. A complete dedicated system exists just for that purpose. Use of SUA airspace can make for a more efficient flight path, if the SUA does not have to be avoided.

The fourth major database input to the ETMS Hub is the Official Airlines Guide (OAG). The OAG contains the schedules of all routine IFR flights for all the airlines using the NAS. The OAG database is updated monthly.

These four main databases are input to the ETMS Hub where they are preprocessed and used to build the databases needed by the ETMS processing algorithms. This preprocessing and related hub internal databases are shown in the center of the Hub section of Figure 4. Geographical maps, airports, airline schedules, aircraft type data and the Grid database are some of the internal databases built.

Figure 3-4 ETMS Functional Diagram

Weather processing is depicted in the upper-left area of the diagram. Weather data is received from the NOAA Environmental Research Laboratory (ERL) and the Weather Systems Incorporated (WSI) corporation. The Hub weather processing system forwards the jet stream data, the precipitation data, and the lightning data out to all TMUs through the Hub weather distribution function. Grid winds are used only internally by the Hub Modeling function.

Two major data processing functions in the Hub are the Traffic Modeling Process and the Traffic Management Process. The Modeling process consists of the Parser (which parses the input flight plans), the Flight Database Processors, and the Traffic Demands Database Processor.

Traffic Modeling begins with a parser that breaks down the content of NAS, DOTS, and Flight Schedule messages into their constituent parts and prepares the data for processing by the Flight Database Processor. The Flight Database Processor maintains an entry for each active, proposed, or completed NAS flight within the past 12 hours. It also updates the flight records when any new flight data arrives.

The third major function of the Flight Database Processor is to distribute data about each aircraft's current situation to other functions within the ETMS.

The Traffic Demands Database Processor monitors air traffic demands in near real time for NAS airports, fixes, and sectors. The Traffic Demands Database processor periodically generates air traffic reports to support Monitor/Alert features in the Remote TSD. It also provides, on-request air traffic reports for any monitored NAS element.

The Hub Traffic Management Functions allow Command Center Traffic Managers to control the flow of traffic by using two main traffic management techniques:

1. Delay of certain flights on the ground to prevent air-borne holding near the destination airport. These are variously known as Estimated Departure Clearance Time (EDCT) programs or Ground Delay programs. The EDCT and Fuel Advisory (FA) files from the Command Center, which appear as input to the Apply Ground Rules box (Figure 3-4 center-area)is the implementation of this concept.

2. Reordering or swapping of flights by departure time when an airline requests changes to their controlled flight departure times because of delays. Refer to Figure 3-4, which shows the Substitution Processing (SI) request messages between the Apply Ground Rules, and the Airlines Dispatch Offices is how the collaboration is implemented.

If the reader wants or needs to learn more about the Hub data processing functions, the *ETMS Software Design Documents (SDD)* supplies additional detailed information.

3.4.2 TMU Remote Functionality

The Remote TMU is depicted at the bottom of Figure 3-4. The Remote TMU is comprised of two major system components. They are the workstation and the File Server. A TMU which is used tactically would normal consist of from one to six workstations and normally two, possibly one File Server. The Command Center has a much larger configuration. The File Server is

illustrated on the left side of Figure 3-4 and the workstation on the right.

The left side of Figure 3-4 depicts how the various NAS Air Traffic facilities interface with the Remote ETMS TMU. These NAS systems interface with their collocated TMUs through the Emulex Module contained in the TMU File Server. It is this Emulex Board interface to the interoperable NAS unit that brings the NAS flight related message traffic from the ATC computer to the Remote TMU. Each TMU then forwards these NAS flight messages to the HUB through the WAN Router and dedicated 56 KBS TCP/IP line.

Each Remote TMU File Server also maintains a set of flights in a locally maintained Flight Tables database. The flights contained in the Flight Tables will be those flights that are currently in the air. This flight table is the source of flights that can be seen on the TSD. Flights appearing on the TSD are airborne only, not future schedules. Future schedules are handled in the HUB Modeling Process.

Occasionally, a traffic management specialist sitting at the TSD will make data requests of the system. The List Server, which is located in the File Server, processes these data requests. The List Server then forwards the request to the centralized Hub data processing system. The Hub then generates the appropriate response, which is returned to the TMU for TSD display.

The TMU File Server also contains the Weather database for use by the local TSD. All the local TSDs will normally be displaying weather data as an integral part of the TSD display.

The Remote TMU workstation is depicted in the bottom-center of Figure 3-4. The Monitor is the focal point of the CHI along with the keyboard and the trackball. A color printing capability is available for color hard copy. The TSD main menu appears in the bottom center of Figure 3-4.

To the right of the Monitor in Figure 3-4, the CDE Remote System Modes appear. These are the major operating modes of the Remote TMU. These CDE Modes, along with the menu that appears on the TSD display, constitute the main functionality available from the Remote TMU.

The major CDE Modes and their functionality are

1. TSD - The Traffic Situation Display (TSD) is an interactive display system that graphically displays current air traffic. The TSD receives flight information from the FTM, weather data from the Weather Server, alert data from the Alert Server Process, and schedule data from the Request Server. When the TSD receives this data, it uses the information to keep current its graphic depictions of flights and flight route information, weather, and alerts.

Using the TSD, the Traffic Management Specialist can communicate with air traffic data processed by the ETMS databases through a graphic display to show many types of information related to air traffic patterns. The display consists of a background map showing geographic or sector boundaries, airports, NAVAIDs, airways, and other elements in whatever combination the Traffic Management Specialist specifies, plus icons representing all the aircraft in the area being displayed. The TSD also enables you to update capacities, schedule information, and GA estimates. These updates are sent to the

central processes at the Volpe Center, where the data is processed.

2. E-mail - The e-mail function constructs and sends messages to the Aeronautical Radio Incorporated (ARINC), the National Airspace Data Interchange Network (NADIN) or another ETMS workstation. There are two types of messages: advisory and general. A message can be constructed in free format, or pre-stored messages can be selected. Only personnel at the ATCSCC can send advisories or send messages to ARINC and NADIN networks.

3. Delay Manager - The Delay Manager provides the Traffic Management Specialist with a selectable set of comprehensive displays that provide assistance in the performance of scheduling demand versus capacity. Delay Manager simulates and evaluates the effects of delayed flights on arriving flights for any airport you choose. This function allows you to evaluate the effects of implementing a ground stop, to examine the status of an EDCT program, and to simulate the releasing of flights from a delay program.

4. TMSH - The Traffic Management Shell allows the operator to invoke a number of ETMS functionalities in addition to whatever else the TMU may be doing. An additional window will normally appear on the display. The Traffic Management Shell is a command interpreter designed to perform efficiently many of the non-geographical functions of the TSD.

5. Pop Notify - Notifies the operator by placing an icon on the screen when a mail message or a report is received by the TMU.

6. ETMS Log - The ETMS Log program can be used by one or more users across a Local Area Network (LAN). It enables you to record operational air traffic activities and other types of data, including standard forms and templates. Then you can use the Log Program to modify, save, or print these forms.

7. RMGR - The Route Manager is a set of programs which provides a service to look up information on airports, NAVAIDs, fixes, preferred IFR routes, and weather reporting locations based on a variety of selection criteria. RMGR provides a menu driven interface. Weather reporting locations are normally airport local weather reporting systems.

8. Sup - The Sup Mode is used to perform verification, fault detection, and isolation. It is primarily a maintenance set of tools used by AF maintenance personnel to verify operability and fault isolate problem situations.

9. Net Mail - Net Mail provides a set of commands that allow the operator to query and monitor ETMS processes. The ATCSCC version of Net Mail, which also runs at the Hub, enables the ETMS hot line staff to monitor and maintain all processes within the ETMS network. Field sites have a restricted version, which limits command access to the local site.

10. SCDT - The SCDT program computes ground delay using a flight list obtained from the ETMS traffic demand database. SCDT generates the EDCT Delay file, which contains a schedule for the flights scheduled to arrive at a designated airport. EDCTs are flight-specific, controlled, departure times for flights known at the time the SCDT program is run. FAs are average delays to be applied to flights that file

flight plans after the SCDT program is run. SCDT also generates FA messages. The SCDT mode exists only at the ATCSCC.

11. Blanket - The Blanket function generates a blanket delay that can be applied to all flights when demand exceeds capacity. Blanket exists only at the Command Center.

12. Autosend - The Autosend function provides the user with the ability to send delays (Selected Controlled Departure Time or Blanket) to centers and airlines. Autosend sends messages to the internal TMU Router, which then connects with the node switch. Autosend exists only at the Command Center.

13. ETMS Help - Help provides online information to the TMU operator.

3.4.3 Integrated System Concept

The right side of Figure 3-4 illustrates the concept of an integrated Hub and Remote TMU system. The Hub Site system component appears in the upper right area, the Remote TMU system component appears in the lower right area, and the External Communications system component appears in the right center area. This integrated system concept illustrates how WAN connects the two sites together for interoperability. A Gateway switch exists at both ends and together, along with the interconnecting communications, they perform the WAN functionality. The Hub site (only one string is shown) illustrates how the software running on different computers interfaces with a node switch that runs on each computer and serves to transmit messages between the different modules. Each computer Node Switch also interconnects through a Local Area Network (LAN) with a Site Switch, which interconnects the various computers connected to the LAN. One of the Node Switches in each LAN also interconnects with the Router (Gateswitch) to perform the WAN interface.

The allocation of processes and switching modules is done in a similar manner at the Hub and TMU Remote units. Each digital computer has a Node Switch, which also interconnects with the Site Switch. One TMU Node Switch also connects to the Gate Switch (Router) for external WAN communications.

For the Remote TMU, the allocations are such that all remote software is situated on each Remote CPU. Therefore, any given computer can be a workstation, a File server, or a backup File server.

The integrated online operational ETMS is a large-scale, software intensive system. The centralized Hub data processing system is interconnected to a distributed network of decentralized remote data processing systems. The concept of Server/Client is evident in both the Remote TMU File Server and workstation architecture and the Hub Remote TMU architecture. ETMS uses the UNIX Network Operating System (OS) throughout.

3.5 ETMS Transition Concept

Figure 3-3 illustrates the ETMS Transition configuration from the current Apollo-based configuration to the new Open Systems configuration. This transition is scheduled to be on going for approximately the first 6 months of 1999. The Apollo configuration and the ETMS OSC configuration will be functioning online concurrently during the transition period.

The Hub will consist of Strings A and B for the Apollo and Open Systems configurations. Synchronization between the two systems will be maintained.

As the fielding of replacement OSC TMUs progresses, the TMU population will gradually change from being predominately Apollo to being predominately Open Systems. To affect the remote site TMU transition, an Apollo TMU will be shut down, then removed. The new Open Systems TMU will be installed and brought online to interface with the Open Systems Hub. The Apollo TMU population will be sequentially replaced with the Open Systems TMU. When the last Apollo TMU has been replaced, the Apollo Hub will be decommissioned.

Figure 3-3 also illustrates the communications interconnection between the Apollo Hub and the Apollo TMUs and also the interconnection between the Open Systems Hub and the Open Systems TMUs. In addition, the various TMU computer configurations are illustrated. Configurations for the typical ARTCC, TRACON, and Control Tower are depicted in Figure 3-3.

4 TMU EQUIPMENT CONFIGURATIONS (DETAILED)

4.1 TMU ARTCCs and CERAPs Configurations

The typical ARTCC configuration, shown in Figure 4-1, consists of the following subsystems. CERAPs sites have the same basic configuration, except that the interfacing systems differ. The Figure 4-1 configuration includes

- At least 5 Open Systems HP 9000 C-Class processors; configured as 3 workstations and 2 file servers. By convention, the two systems labeled WKSTN01 and WKSTN02 are the primary and backup file servers. ETMS processors include
  - 256 MB memory
  - Compact Disk-Read Only Memory (CD-ROM) drive
  - One 9-GB, Ultra-Wide, Single-Ended Small Computer System Interface (SCSI) Disk
  - Localization kit (keyboard, manual, power cord
  - Trackerball Trackball, labeled Massey
  - HP-UX Operating System (OS)
  - An HP 21" graphics monitor. Most workstations have a single monitor. However, with the addition of a dual graphics card, a second monitor can be connected, as shown in Figure 4-1 WKSTN03
  - Either 2 or 4 EMULEX cards in the file servers of those sites that interface with the HCS and/or other interfaces. The other ARTCC/CERAPs interface systems include the Oceanic Display and Planning System (ODAPS), the EARTS, the OCS, and the Offshore Flight Data Processing System (OFDPS).

  All ETMS TMUs located at ARTCCs interface with the Host digital computer. Rokonkoma, NY and Oakland, CA TMUs also interface with the ODAPS (Oceanic systems) and have the four cards. The Anchorage TMU interfaces with EARTS and OCS. The Honolulu, HI CERAP interfaces with EARTS and OFDPS.
- HP DDS-3 Desktop Digital Archive Tape (DAT) drive attached to each workstation and file server through the SCSI serial port
- APC 2200s Smart-Un-interruptible Power Supply (UPS) backing up the file servers and workstations for the majority of sites, which do not have critical power. For those sites that do have critical power, the addition of a power filter to the configuration is currently To Be Determined (TBD).
- Two HP 1600 CM color inkjet printers
- Two CISCO 10/100Base-T dual-speed hubs with either 12 (112T) or 24 ports (124T). Note that only sites with at least 7 workstation/file server processors have the 24-port hubs.
- Two CISCO 1601 routers, only one of which is actively communicating with the WAN at one time. Each site's connection to the WAN is either Leased Inter-facility NAS Communication System (LINCS)-leased landlines or FTS-2000 connections. LINCS can be either LINCS A (digital) or LINCS B (analog). For analog connections, either the Codex 3512 modem or the ATT 56/64 modem is used.

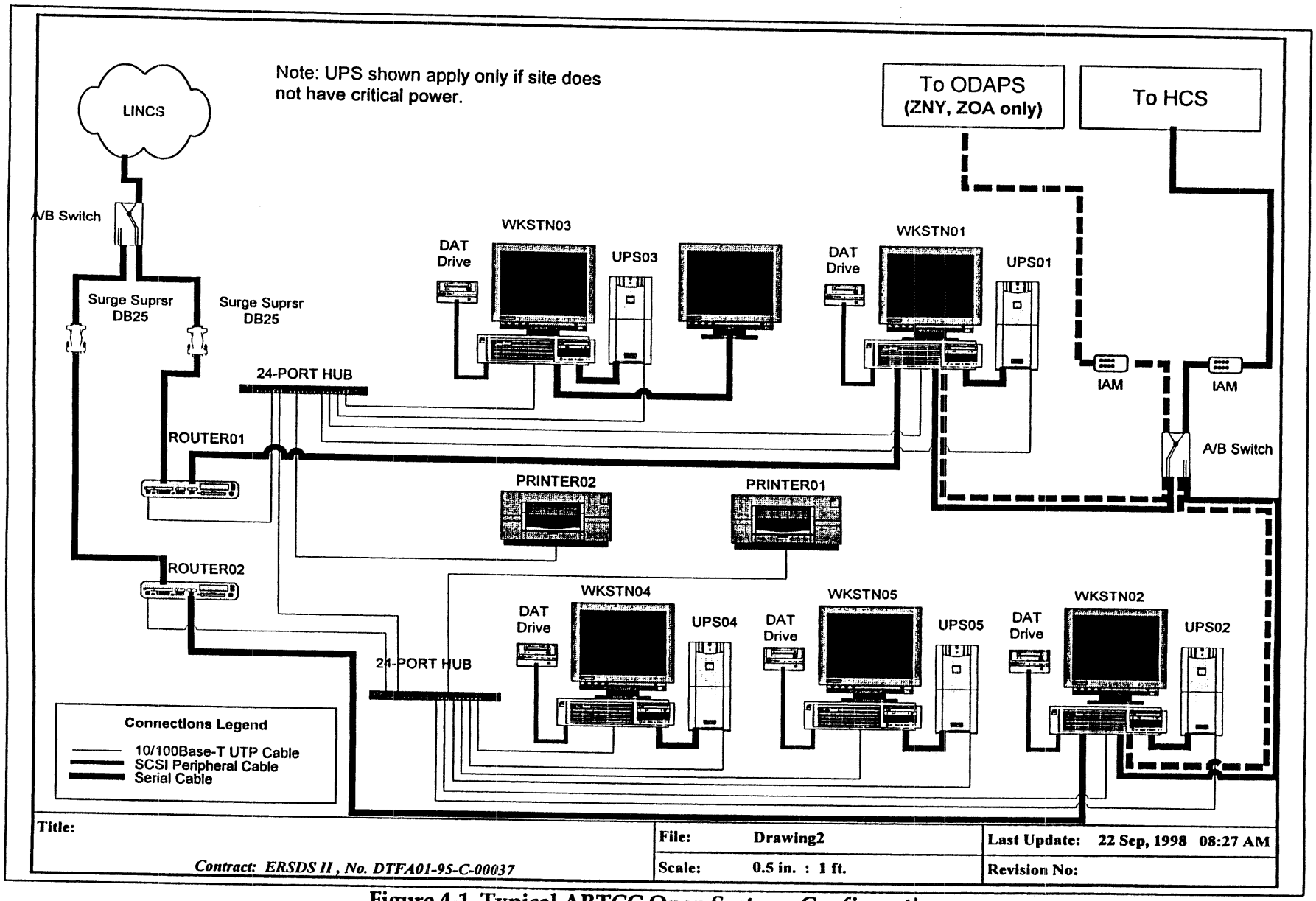


Figure 4-1 Typical ARTCC Open Systems Configuration

- A/B switches for switching both file servers and the routers back and forth from the primary to backup units
- DB25 Surge Suppressors are shown in the Figure 4-1 s part of the interface to the external LINCS communications. Also depicted in Figure 4-1 are In-line Activity Monitors (IAMs). IAMs are used to monitor the ETMS interface to the Host computer System and to the ODAPS (ZNY and ZOA systems only).

New York, Houston, Leesburg, and Oakland ARTCCs are exceptions to the standard configuration of five, HP 9000 C-Class processors. New York and Oakland have 7, and Leesburg has 9. The 2 additional workstations at New York and Oakland are used by the ATCs in the oceanic sectors. Because of the additional processors, these sites use 24-port rather than 12-port hubs.

4.2 TMU TRACON, Tower, and Regional Office Configurations

Figure 4-2, TRACON (With Tower) TMU Open Systems Physical Block Diagram, and Figure 4-3, Regional Office Configuration, show typical configurations.

Some of the main differences are

- Both have fewer workstations than the ARTCCs and CERAPs. Most TRACON configurations (with or without towers) have 4 processors - 2 file servers and 2 workstations. The exceptions are that New York, Southern California and Northern California have 7 processors (2 file servers and 5 workstations), and New York has 5 additional monitors.

  Towers that do not reside with a TRACON have 3 processors - the redundant file servers and 1 workstation and 1 printer. Their LAN/WAN configuration is just like ARTCCs and TRACONs, with the dual routers and 2 hubs. Towers without TRACONs are located at Newark, Kennedy, Los Angeles, San Francisco, Chicago, LaGuardia, and Dallas/Ft. Worth.

- The Regional Offices has a single Hub, a File server, a Workstation, and a Router
- Two Media Converters are added for TRACONs with a tower
- The interfacing systems for the TRACONs are the Automated Radar Terminal System (ARTS-IIIE) and the future ARTS-IIIE replacement, the Standard Terminal Automation Replacement System (STARS).

4.3 TMU System Components

The basic ETMS components were introduced in the ARTCC, TRACON with Tower, CERAP and Regional Office configurations. This subsection further elaborates on some of the TMU system configurations and components.

The TMU file server is illustrated in Figure 4-4. Dual file servers are each connected to the TMU hub via cables. One file server is online and the other is in a backup status. The file servers can be switched via the Sup Mode>System>Switch File Server command.

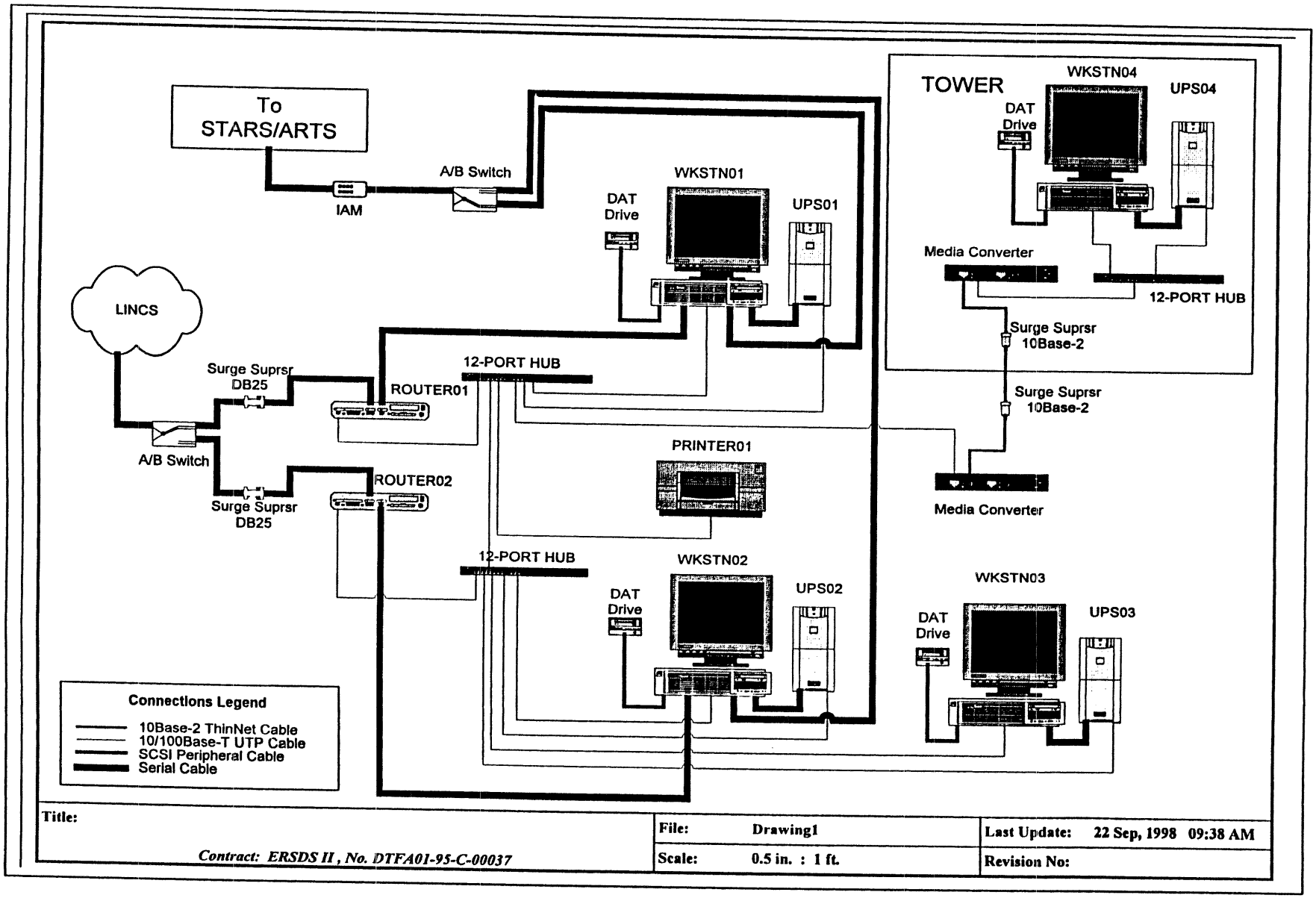


Figure 4-2 Typical TRACON (With Tower) TMU Open Systems Configuration

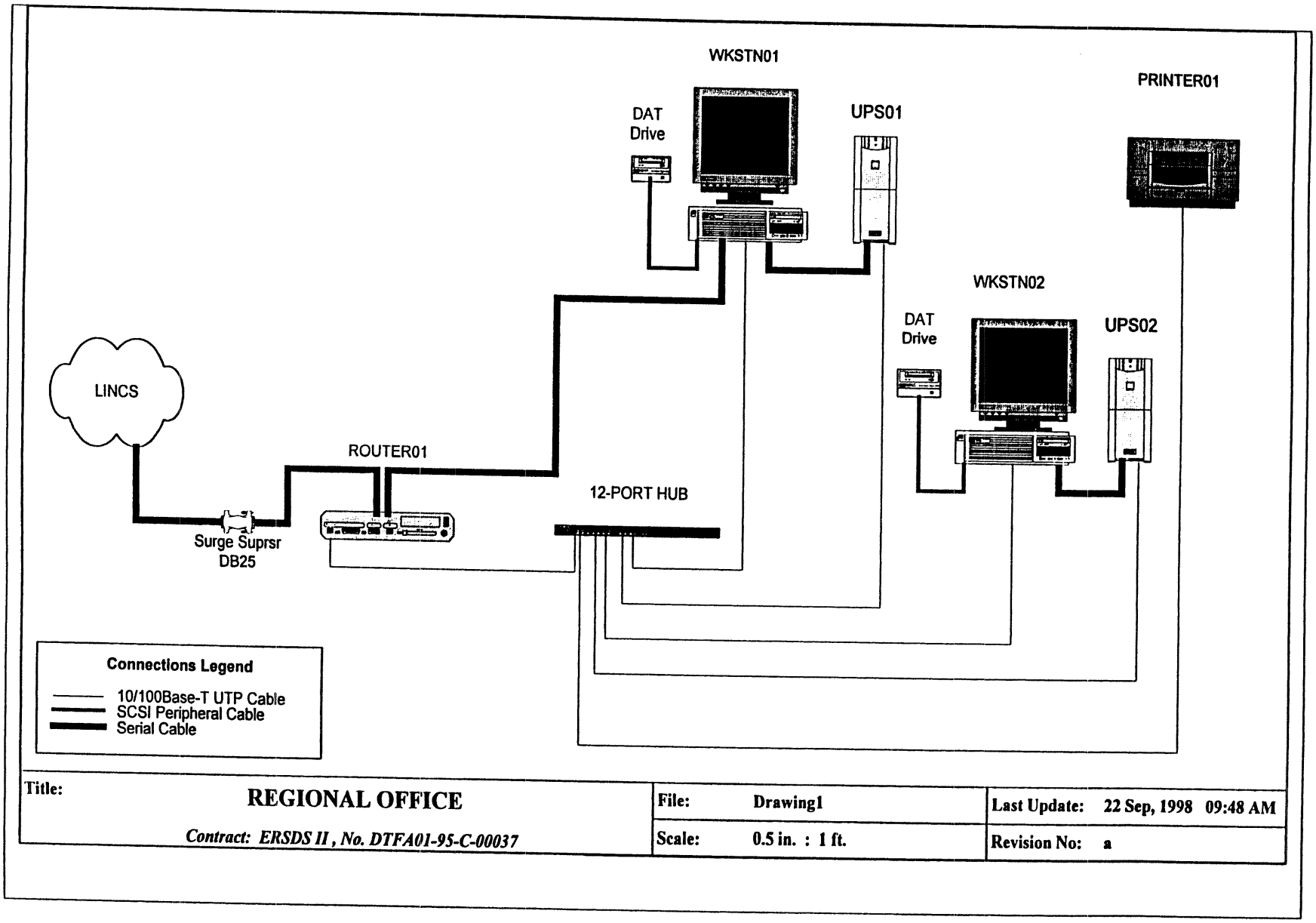


Figure 4-3 Regional Office Configuration

The TMU primary file server and backup file server provide multi-functionality as communication devices to connect the Host with the TMCCC. A dual-port input A/B switch connects the appropriate file server to the multiplexed communications link to the TMCCC. The Regional Offices have only one file server

The Emulex communication cards resident in the file servers relay messages to the Host computer and provide ARTCC-specific flight data for generation of the composite TSD data products the TMCCC distributes.

Figure 4-4, File server Configuration, shows front and rear views of the file server. The version shown has the 2 EMULEX cards and 4 ports for those TMUs that interface with more than one external system.

Workstations have the same specifications for memory and disk drive size. The main differences in the ports and internal cards are that workstations and some file servers would not have EMULEX cards, and workstations could also have a second graphics card for driving a second monitor.

Figure 4-5 depicts the 24-port Hub. The 12-port hub looks the same as Figure 4-5 with only the corresponding reduction in ports. Figure 4-6 depicts the CISCO 1601 router. Figure 4-7 depicts the American Power Conversion (APC) Smart UPS. Puss are only used if a site does not have critical power.

4.4 ETMS Auxiliary Equipment

TMS relies on the following auxiliary equipment.

1) The Computerized Voice Reservation System (CVRS) workstation provides a terminal and a printer for control of the ARF. The CVRS uses four toll-free numbers with rollover capability and multiple circuits to provide the service.

2) The TMCCC receives weather data from Weather Services International (WSI) located in Boulder, CO. This weather data is sent through a 56 KBPS landline to the TMCCC for distribution to TMU sites through the ETMS communications WAN.

3) The National Airspace Data Interchange Network (NADIN) interfaces with the TMCCC. This allows CFC to send output through the workstations and receive input on the AFTN printer.

4) The Aeronautical Radio, Incorporated (ARINC) network also interfaces with the TMCCC, providing oceanic track updates and allowing Central Flow Control (CFC) to send output through the workstations and receive input on the ARINC network printers.

5) The LINCS communication network is a leased service that provides communications across landlines to TMU facilities. This communication network functions at a rate up to 64 KBPS.

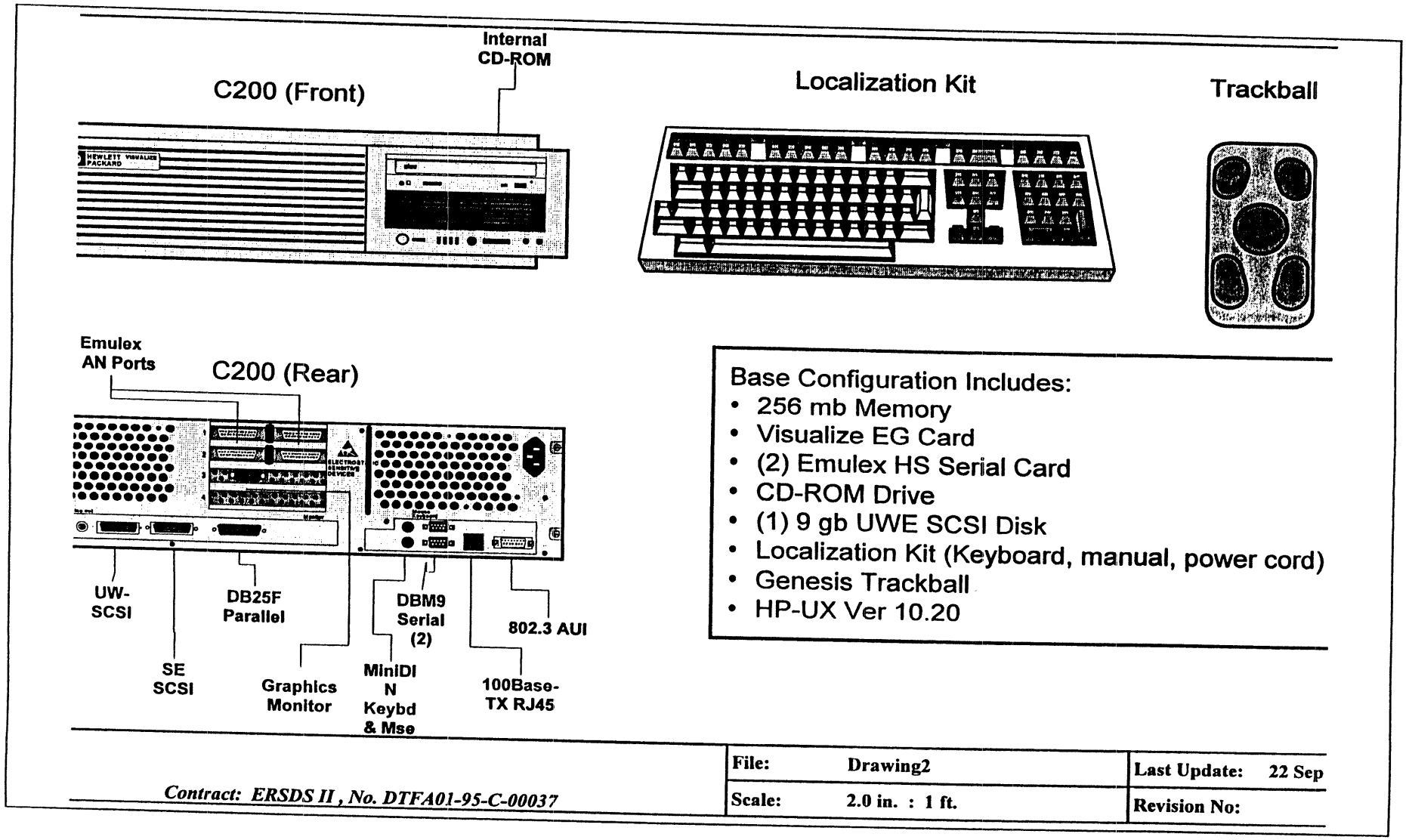
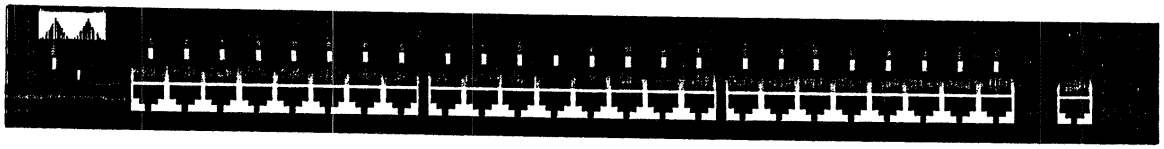


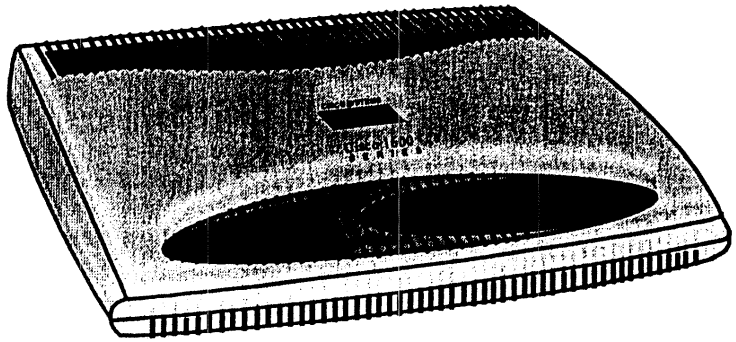
Figure 4-4 File server Configuration



Title	File: Drawing3	Last Update: 22 Sep 1998 11:03 AM
Contract: EDSIS II, No. DTEA01-95-C-00037	Scale: 4.0 in : 1 ft.	Revision No:

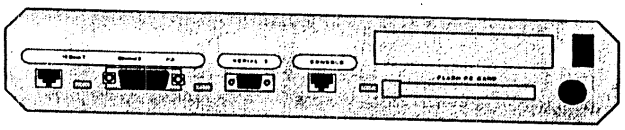
Figure 4-5. 24-Port Hub

Cisco 1601 Router (Front)



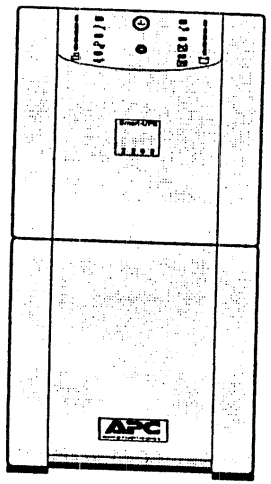
Cisco 1601 Router Configuration Includes:
- 4 mb DRAM memory
- 6 mb Flash memory (PCMCIA card)
- (1) Ethernet Port (10BaseT)
- (1) WAN Port (Synch/Asynch Serial)
- RS-530 Cable

Cisco 1601 Router (Rear)



Title:	File: Drawing1	Last Update: 22 Sep, 1998 11:08 AM
Contract: ERSDS II , No. DTFA01-95-C-00037	Scale: 4.0 in. : 1 ft.	Revision No:

Figure 4-6. Cisco 1601 Router



APC SU2200 Floor Standing UPS
Configuration Includes:

- Smart-UPS Model SU2200NET
- Power-Chute S/W
- 20 amp Optional Backplate (SU029)
- SNMP Adapter

Title:	File: Drawing2	Last Update: 22 Sep, 1998 11:09 AM
Contract: ERSDS II , No. DTFA01-95-C-00037	Scale: 2.0 in. : 1 ft.	Revision No:

Figure 4-7. APC Smart UPS

b. This section addresses the theory of operation of the TMS auxiliary systems.

1) The ARF network aids the management of traffic at high-density traffic airports (HDTA). General aviation (GA) reservations to HDTAs must be requested of and approved by the ARF. Normally, this is accomplished when pilots call in to the CVRS to file their reservations. FMSs can then review these reservations from the ARF terminal. They also manage the demand by programming the system with the number of permitted reservations. When necessary, they can manually enter pilot reservations.

2) The NADIN is used to relay international meteorological and aeronautical data. The FAA Service B communications between ARTCCs and flight service stations is also available on NADIN. CFC uses this network to send and receive flow control advisories to and from ARTCCs and the Flight Service System (FSS).

3) The ARINC network is used to send flow control advisories to the airlines and to receive notice of flight plan changes from the airlines on the printer.

5 ETMS TMU VERIFICATION MAINTENANCE CONCEPT

5.1 THE CONCEPT

Verification is an ongoing process wherein all of the system's capabilities, features, and functionality are confirmed to be operational in a manner deemed to be free of hardware and software degradations.

5.2 Types of Verification.

5.2.1 Service Level.

This level of verification is for the overall CFC processing of TMS management information made up of the automation hardware and software systems. This type of verification is the final level and requires that the next lower level of verification be current. Services use systems, but services includes the system method of providing people with the use of something. An example of service would be Traffic Management. Service. Traffic Management Service includes the concept of how the system is used, i.e. usage.

5.2.2 System Level.

This level of verification provides the basis for the service level. In turn this level of verification is, in part, based on the element, equipment and communications.

5.3 Verification Responsibility.

Verification responsibility will be assigned to appropriate technical personnel in accordance with the requirements.

Verification responsibility designations included in the verification parameter tables are for general guidance only. It is recognized that circumstances will arise that will necessitate special designations by the sector manager or other personnel having sufficient and appropriate expertise to perform technical verification of service and system performance. Special designees must comply with the requirements of the Airway Facilities Maintenance Personnel Verification Program

The objective of ETMS TMU field maintenance and field maintenance support activity is to provide verification of a fully operable system. Maintenance Verification is a concept wherein both the routine and corrective maintenance processes are directed at maintaining this fully operational ETMS.

The transition to an Open Systems TMU baseline entails an all new configuration except for application program software. This all new equipment baseline entails some significant changes to the current TMU maintenance activity.

Table 5-1 delineates the top-level viewpoint of this TMU Open Systems maintenance program.

Table 5-1 TMU Open Systems Maintenance Concept

System Subsystem LRU Components	Preventive Maintenance And Fault Isolate	Remove/ Replace/Test And Repair (as required)*	Depot Supply Support
ETMS			
HP 360 Workstation			
CPU	AF	Hewlett-Packard*	Hewlett-Packard
Keyboard	AF	Hewlett-Packard*	Hewlett-Packard
Regular Monitor	AF	Hewlett-Packard*	Hewlett-Packard
External Archive Tower(ATCSCC) (1)	AF	Hewlett-Packard*	Hewlett-Packard
External Tape Drive (DAT)	AF	Hewlett-Packard*	Hewlett-Packard
HP Color Printer	AF	Hewlett-Packard*	Hewlett-Packard
Ink jet cartridges	AF	AF	FDC
Peripheral Equipment			
High Bright Monitor(Twr; if provided)	AF	Hewlett-Packard*	Hewlett-Packard
Trackball	AF	AF	FDC
Extended Monitor Cable	AF	AF	FDC
Extended Keyboard Cable	AF	AF	FDC
Console Port Cable	AF	AF	FDC
Video splitters	AF	AF	FDC
Network Routers (Cisco 1601)	AF	AF	FDC
12 & 24 Port Ethernet Hubs	AF	AF	FDC
APC UPS - 1400 VA	AF	AF	FDC
A/B mechanical switch	AF	AF	FAALC
Surge Suppressor 100BaseT (RJ-45)	AF	AF	FAALC
Surge Suppressor ThinNet (BNC)	AF	AF	FAALC
Surge Suppressor RS-422 (DB-25)	AF	AF	FAALC
Media converter	AF	AF	FAALC
Ethernet Repeaters	AF	AF	FAALC
Inline Activity Monitor	AF	AF	FAALC
LINCS Cable Assy (Demarc - Rtr A/B)	AF	AF*	
Plenum Cable, Shielded	AF	AF	FAALC
Connectors (DB-25)	AF	AF	FAALC
FTS-2000 Cable Assy (Mdm - Rtr A/B)	AF	AF*	
Plenum Cable, Shielded	AF	AF	FAALC
Connectors (DB-25)	AF	AF	FAALC
Crossover Cable Assembly	AF	AF*	
Plenum Cable, Shielded	AF	AF	FAALC
Connectors (DB-25)	AF	AF	FAALC
NAS Interface Cable Assemblies (External - A/B switch & A/B - Emulex)	AF	AF*	
Plenum Cable, Individually Shielded	AF	AF	FAALC
Connectors (DB-25)	AF	AF	FAALC
Local Area Network Cable Assemblies	AF	AF*	
100BaseT Cable	AF	AF	FAALC
ThinNet cable	AF	AF	FAALC
Connectors (RJ-45)	AF	AF	FAALC
Connectors (Coax)	AF	AF	FAALC
Installation – Test Aids			
Multi-network Cable Testers	N/A	N/A	FAALC
Cartridge Tapes			
4 GB DAT – DDS2, 120m	N/A	(2)	FAALC
Cleaning Cartridge for DAT	N/A	(3)	FAALC

(1) Training to be provided by FDC at time of installation.

(2) No repair function, tapes will be removed as required.

(3) No repair function, cleaning tapes will be used during preventive maintenance.

Hewlett-Packard: 1-800-633-3600, Federal Data Corporation: 1-800-955-UNIX ext. 3446

6 TMU ROUTINE VERIFICATION MAINTENANCE

6.1 GENERAL OVERVIEW.

This chapter establishes all the maintenance activities which are required for the ETMS TMU on a routine basis. The two major categories of Routine Maintenance are Periodic and Non-Periodic. The schedules for their accomplishment and the detailed procedures themselves have been included. Refer to the latest edition of Order 6000.15 for additional general guidance.

The detailed procedures include, where applicable, the standards and tolerances to be used.

The following performance checks and maintenance tasks are not to be taken as the minimum work required for proper maintenance, rather as the maximum interval permitted between tasks. Refer to the latest edition of Order 6000.15 for guidance

It is to be understood that, for a given period, the tasks listed for that period and all more frequent periods are to be performed at that time. For instance, on an anniversary, the annual, semiannual, quarterly, monthly, weekly, and daily tasks shall all be performed. Maintenance procedures shall be performed under conditions that duplicate, as closely as practicable, those present during normal operation

Objective. This section conveys types of routine maintenance verification, verification responsibilities, basic guidelines, and performance checking procedures essential to the technical verification of the services, systems, and equipment that comprise the TMS; a large-scale, complex system providing automation capability in support of the FAA air traffic control mission.

General. A substantial portion of the AF maintenance mission is dedicated to the determination of the performance status of the overall functional capability or service being provided to the user. Some performance checking is accomplished on-line by using manual techniques, and some must be accomplished using off-line diagnostic programs. Periodic use of performance check procedures sets the desired confidence level in system performance and also reinforces the AF technician's understanding of the system.

Procedures. Unique, specialized developed procedures not suitable for inclusion in other maintenance documents are included in this section to standardize performance checking actions, promote better repeatability, and facilitate trend analysis, as well as support verification.

FAA Form Entries. Order 6000.15 contains policy, guidance, and detailed instructions for field use of the Technical Performance Record (TPR), as applicable to the TMS. Entries shall be made in accordance with the instructions published in Order 6000.15. Figures 6-1, and 6-2 contain samples of FAA Forms 6000-8.

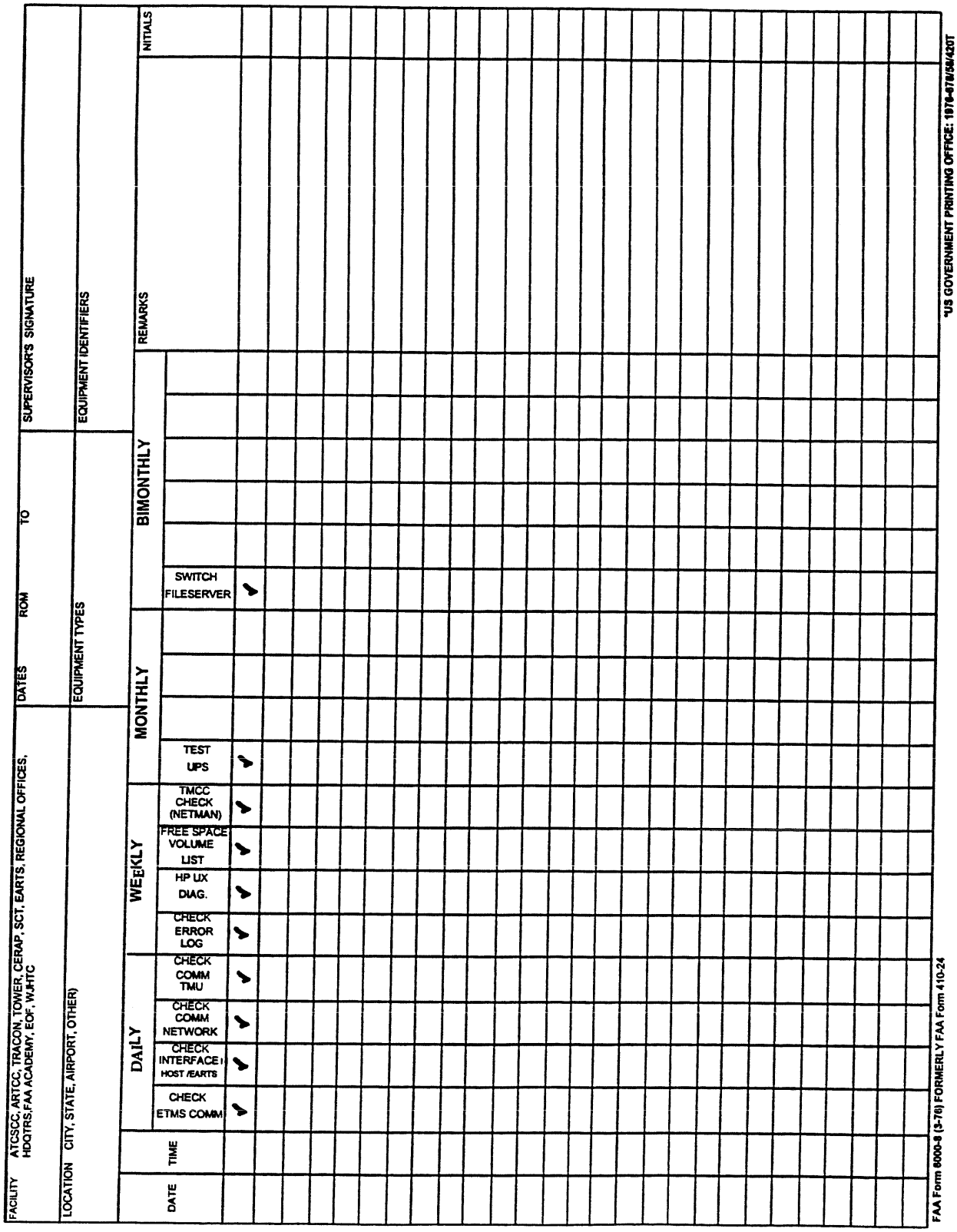


Figure 6-1 Technical Performance Record (Page 1 of 2)

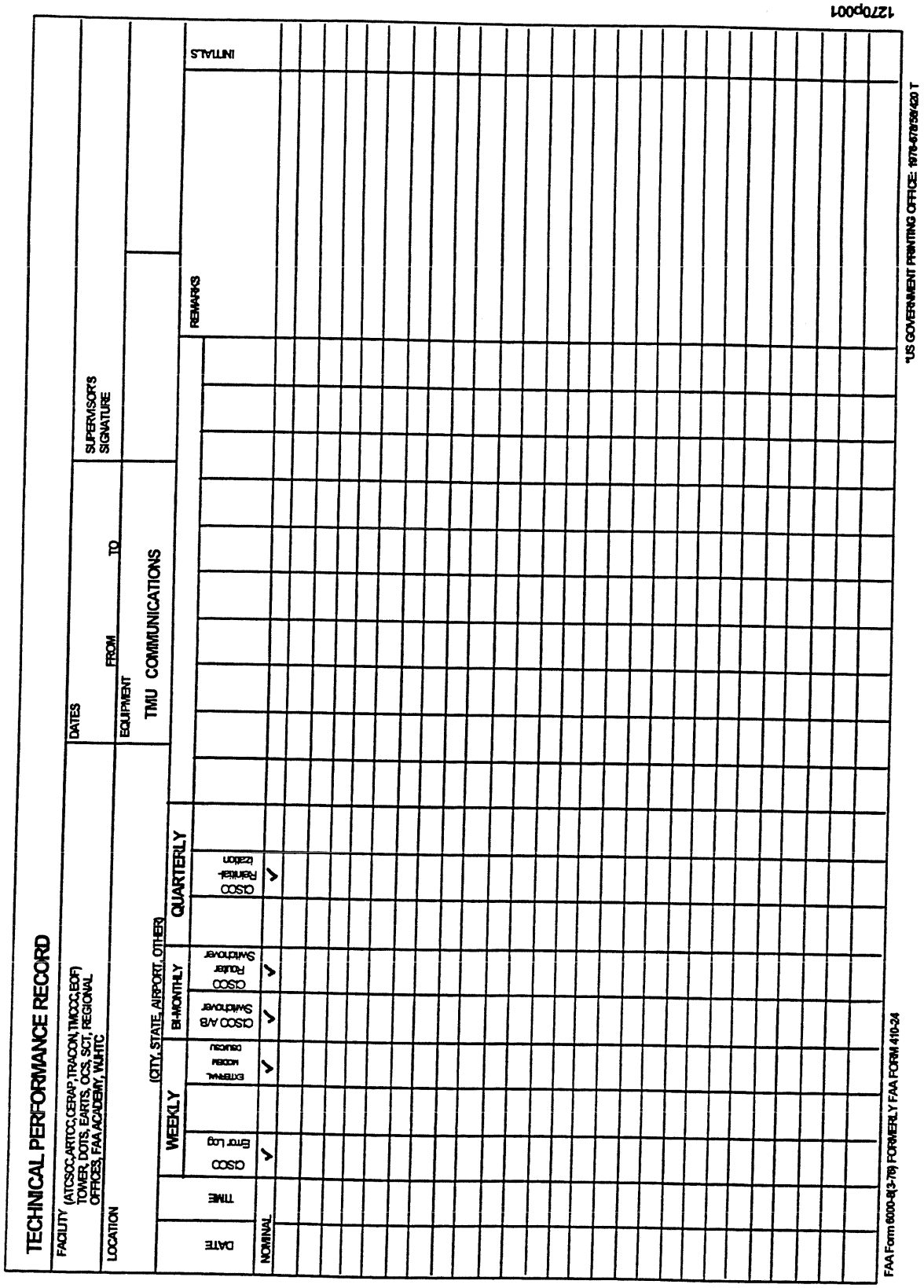


Figure 6-2 Technical Performance Record (Page 2 of 2)

6.2 Periodic Performance Checks

Periodic Performance Checks are those performance checks made on a routine, repetitive, basis.

6.2.1 Overview

The Periodic Performance Checks as outlined in this document provide a degree of TMS verification. They are specific checks made to assure operability of certain ETMS TMU system component(s). Periodic Performance Checks do not, as of this version of the document, provide a complete verification of the TMU system. This will be done in a later versions of this order. The Periodic Performance Checks contained herein provide assurance that equipment components, such as the tape station and the File Servers work. Appendix A illustrates the approach to be taken to achieve full TMS verification.

The schedule for Periodic Performance Checks is contained in the following table:

Table 6-1 Periodic Performance Checks Schedule

Performance Checks	*Maintenance Procedures*
6.2.1.1 DAILY.	
TMU Network Communications Operability Checks *(All Sites Having a TMU)* (FAA Form 6110-9 Item)	
(1) TMU – TMCCC Communications Check	6.2.2.4
(2) LAN Ethernet ping and netstat Checks	6.2.2.6, **Error! Reference source not found.**
(3) TMU – TMCCC - TMU Communications Check	6.2.2.5
(4) ATCSCC Communication Check	6.2.2.14
TMU Operation *(All sites Having a TMU)* (FAA Form 6110-9 Item)	
(1) TMU System Error Logs Check	6.2.2.8
(2) Obsolete Files Deletion	TBD
TMU - NAS Computer Communications Checks *ARTCC, CERAP, selected TRACONs)* FAA Form 6160-9 Item	
(1) TMU File Server to HOST/ARTS communications Check	6.2.2.15

Performance Checks	*Maintenance Procedures*
6.2.1.2 WEEKLY.	
TMU Operation Checks *(All sites)* (FAA Form 6110-9 Item)	
(1) HP UX Diagnostic Check	6.2.2.3
(2) List Volume Free Space	6.2.2.10
TMU CISCO 1601 Router Checks *(All sites)* (FAA Form 6110-9 Item)	
(1) Cisco 1601 Router Operability Check	6.2.2.9
(2) CISCO 1601 Router Error Log Check	6.2.2.11
6.2.1.3 MONTHLY.	
TMU UPS Operation Check *(All sites)* (FAA Form 6110-9 Item)	
(1) UPS Availability Test	6.2.2.13
6.2.1.4 BIMONTHLY. (every 2 months)	
TMU Communications Switchover Checks *(All sites configured with standby file servers and standby routers))* (FAA Form 6110-9 Item)	
(1) TMU File Server Switchover Check	6.2.2.1,6.2.2.2
(2) Spare CISCO Router A/B Switchover Check	6.2.2.17
(3) Spare CISCO 1601 Router Switchover Check	6.2.2.16

Performance Checks	*Maintenance Procedures*
6.2.1.5 QUARTERLY.	
TMU Router Re-initialization (All sites configured with standby Router) (FAA Form 6110-9 Item) (1) Standby CISCO 1601 Router Re-initialization	6.2.2.12
6.2.1.6 SEMIANNUALLY – (RESERVED).	
6.2.1.7 ANNUALLY – (RESERVED).	

6.2.2 DETAILED PROCEDURES

The detailed procedures which follow are to be used by AF personnel as part of the overall TMS verification.

6.2.2.1 TMU FILE SERVER SWITCHOVER CHECK (WKSTN01 TO WKSTN02)

a. Objective. This check is performed in order to verify that the backup file server in a TMU has been maintained and is a valid backup to the operational file server.

b. Discussion. In the event that the operational file server's performance is degraded to the point that it can not sustain data transfer or the flight table database becomes corrupted, TSD operations can switch to the WKSTN02. Following the completion of the switchover script, the TMU workstations will resume displaying TSD data. The script used to perform this file server switchover is comprised of stages. Each stage performs a logical group of functions pertaining to the switchover process.

c. Test Equipment Required. None.

d. Conditions: The check shall be performed while the TMU is under a typical operational load.

e. Detailed Procedure.

(1) On WKSTN01, perform the following. Select the ETMS icon, then select the Sup Mode icon, this will display the Sup Mode interface.

(2) In the Sup Mode interface select the Utilities button located at the top of the interface. This will display a listing of scripts.

(3) Double click the left trackball button to highlight the switch file server script. Then select the Execute button

(4) A message will appear as follows:

"This script will attempt to configure //WKSTN02 to be the active file server and //WKSTN01 as the backup file server." Do you want to continue?

(y/n).

(5) Respond by typing "y" then press "return." Respond with "n" only If your database has been corrupted, normally "y" will always be the selection.

(6) You will be prompted to:

"Call the ETMS Operations on 617-494-2556 or 2557. TELL THEM THAT YOUR FILE SERVER IS NOW WKSTN02. ASK THEM TO REDIRECT THE MONITOR ALERT AND WEATHER DATA TO //WKSTN02. ADVISE THEM HOW LONG //WKSTN02 WILL BE THE PRIMARY FILE SERVER".

(7) The following prompt will appear:

****

Please ensure that the file server selection

**switch is properly positioned to select **

//WKSTN02 as the primary file server. AFTER

**POSITIONING THE SWITCH, PRESS **

**<RETURN> TO CONTINUE **

a) FILE SERVER SELECT SWITCH POSITIONS:
   A = WKSTN01
   B = WKSTN02 ===SELECT THIS POSITION

C = LOOP-BACK
D = N/A

b) Press the <RETURN> key.

(8) A number of information processes will be displayed as to processes starting and being stopped.

(9) When the file server switch is completed a message will appear that says:

*** SWITCH_FILE SERVER COMPLETED***

(10) Go to each workstation running TSD and perform one of the following:

a) QUIT EACH TSD WINDOW AND RESTART EACH TSD WINDOW.
b) E <"> IN EACH TSD WINDOW (double quote).

(11) On WKSTN01, perform the following. At the Display Manager window and with the cursor at the COMMAND: prompt, type the following:

Select the Exit button on the CDE panel

(12) Log into the TSD as a user.

(13) WKSTN01 may now be used as a workstation or may be SHUT down.

(14) Log-off both file servers by selecting the Exit button on the CDE panel.

6.2.2.2 TMU FILE SERVER SWITCHOVER CHECK (WKSTN02 TO WKSTN01).

a. Objective. This procedure is performed to return to the standard operating configuration.

b. Discussion. Same as paragraph 6.2.2.1 b.

c. Test Equipment Required. None.

d. Conditions. Same as paragraph 6.2.2.1.d.

e. Detailed Procedure. Same as paragraph 6.2.2.1e except replace WKSTN02 for WKSTN01; replace WKSTN01 for WKSTN02; and replace step 6.2.2.1 e (7) a) with the following:

Turn the TSD data A/B switch to position "A" (WKSTN01).

6.2.2.3 HP UX DIAGNOSTIC CHECK.

a. Objective. This check is performed in order to verify that all workstation subsystems remain operational even under test conditions. *Note: This check may be completed in an automated utility script (CRON) but the results must be verified by the AF Maintenance Engineer.*

b. Discussion. None.

c. Test Equipment. None.

d. Conditions. The check shall be performed with the workstation in the network.

e. Detailed Procedure. TBD

6.2.2.4 TMU TO TMCCC COMMUNICATIONS CHECK

a. Objective. This check is performed in order to verify that the TMU is communicating with the TMCCC.

b. Discussion. When an operational workstation is on-line, its display may contain icons, which identify which TMUs are off-line. When a TMU is experiencing communication difficulties or a TMU is not communicating with the TMCCC, a respective TSD red icon will be displayed for that TMU on all operational workstations. When a TMU is operational and communications are nominal, no icon will be shown.

c. Test Equipment Required. None.

d. Conditions. The TMU workstation from which the check is being made must be on-line and have nominal communications with the TMCCC. The target TMU must also be on-line and have nominal communications with the TMCCC.

e. Detailed Procedure. Observe that there are no communication failure "Ghostbusters" icons on for a TMU you are trying to communicate with.

6.2.2.5 TMU TO TMCCC TO TMU COMMUNICATIONS CHECK

a. Objective. This check is performed in order to verify that the network is communicating to all user sites

b. Discussion. The field sites have the capability to monitor and report on the status of all communication links to the user sites. A dedicated program "WATCHDOG" has been established to record and display any communication warning or failure messages.

c. Test Equipment Required. None.

d. Conditions. The file server status shell must be on-line in the mode to display the "WATCHDOG" program information.

e. Detailed Procedure. On a file server status shell display, observe that there are less than 20% communication failures. Clicking on the help icon will display a key for interpreting the "Watchdog" information. Further detailed information interpreting the "WATCHDOG" monitor may be found in the functional description distributed through ETMS Tech Note.

6.2.2.6 LAN ETHERNET ping CHECK.

a. Objective. This check is performed in order to verify that the Ethernet network is communicating reliably. Note: This check may be completed in an automated utility script (CRON) but the results must be verified by a technician.

b. Discussion. Information on how the ping command works can be obtained by typing man ping in the command line of a ddterm window. The Unix Ping command will exercise the Ethernet network communications and poll each active node on the LAN. It attempts to communicate with each node and then reports the statistics of how many errors occurred while trying to communicate.

c. Test Equipment Required. None.

d. Conditions. The TMU workstation from which the check is being made must be on-line in the user mode and displaying a shell prompt.

e. Detailed Procedure.

(1) At the shell prompt, type the command:

lshosts

(2) Check for reliable operation by noting that all nodes expected to be active are listed and that the number of transmit errors for each node is zero.

6.2.2.7 LAN ETHERNET netstat CHECK.

a. Objective. This check is performed in order to verify that the Ethernet network is communicating reliably. Note: This check may be completed in an automated utility script (CRON) but the results must be verified by a technician.

b. Discussion. Information on the details of how the netstat command works can be obtained by typing man netstat in the command line of a ddterm window. The netstat command will exercise the Ethernet network

communications and provide network statistics for each active node on the LAN. If any nodes respond to the command is an indication the 802.3 network is functioning. However, all connected nodes should respond when polled with this command.

c. Test Equipment Required. None.

d. Conditions. The TMU workstation from which the check is being made must be on-line in the user mode and displaying a shell prompt.

e. Detailed Procedure.

At the shell prompt on each workstation type the command:

netstat -I -a -config

Check for reliable operation by noting that all statistics are listed and active.

6.2.2.8 TMU SYSTEM ERROR LOGS CHECK.

a. Objective. This check is performed in order to verify that the workstation is not accumulating system errors, which may be undetected by the operator. *Note: This check may be completed in an automated utility script (CRON) but the results must be verified by a technician.*

b. Discussion. The error log maintains a log of all system errors that the processor's operating system is able to detect. A list of the system errors reported in the log follows below.

(1) System startups

(2) Disk errors

(3) ECC errors

(4) Parity errors

(5) System shutdowns

(6) System crashes

(7) Multibus time-outs

(8) Spurious bus errors

The log file is written as a ring buffer. Since entries are therefore eventually overwritten, it is important that the log be checked regularly.

c. Test Equipment Required. None.

d. Conditions. The workstation/file server must be logged into the user mode.

e. Detailed Procedure.

(1) At the shell prompt, type the command: cd /var/adm/syslog

(2) At the shell prompt, type the command: dtpad syslog.log

(3) Check that system errors are not accumulating.

(4) Call system administrator if errors accumulate as noted above.

6.2.2.9 CISCO 1601 ROUTER OPERABILITY CHECK

a. Objective. This check is performed to verify that the CISCO 1601 Router is operating and connected.

b. Discussion.

c. Test Equipment Required. None.

d. Conditions. None.

e. Detailed Procedure.

(1) TBD

6.2.2.10 LIST VOLUME FREE SPACE.

a. Objective. This check is performed to verify that there is adequate free space available on the disk for each TMU workstation and file server. *Note: This check may be completed in an automated utility (CRON) script but the results must be verified by a technician.*

b. Discussion. Over a period of time, the free disk space is utilized by the

operating system to store logs, reports, data files, and startup scripts. Some of this data becomes obsolete and should be removed periodically. If there is no space available for the operating system to utilize, the operating system performance will start to degrade, affecting the operation of the TSD software. If there is less than 15% free space available, notify your TMS Administrator that an abnormal condition exists.

c. **Test Equipment Required.** None.

d. **Conditions.** None.

e. **Detailed Procedure.**

(1) At the shell prompt, issue the command: bdf

(2) Verify that free disk space is greater the 15% for the root volume (/), if less 15%; notify your System Administrator.

6.2.2.11 CISCO 1601 ROUTER ERROR LOG CHECK

a. **Objective.** This check is performed to verify that the Router Error Log File contains a chronology of router events and that any error message entries are properly investigated.

b. **Discussion.** The log file maintains a chronology of activities and events experienced by the router. It also contains error messages that may have been generated by the router.

c. **Test Equipment Required.** None.

d. **Conditions.** None.

e. **Detailed Procedure.**

(1) Telnet into the router.

(2) Select the Log display mode desired.

(3) Examine the contents of the log file.

(4) Investigate any abnormal or suspicious entries.

(5) Exit the TELNET Mode.

6.2.2.12 STANDBY CISCO 1601 ROUTER RE-INITIALIZATION

a. **Objective.** This check allows the router to perform self-diagnostics that are performed only on reboot. It provides assurance that the router has not developed any internal problems that would otherwise go undetected.

b. **Discussion.** By periodically down-sequencing the router and then rebooting, internal reboot type diagnostics will be run. If diagnostic errors occur during the reboot, then the router should be replaced.

c. **Test Equipment Required.** None.

d. **Conditions.** None.

e. **Detailed Procedure.**

(1) Make certain the router that is to be down-sequenced is in the standby position.

(2) Down sequence the router by turning the power switch to the off position.

(3) Reboot the router by turning the power switch to the on position.

(4) Examine the Router Error Log file by telneting into the error file and examining the contents.

(5) Investigate any abnormal error log entries. Replace the router if the error messages so warrant the action.

6.2.2.13 UPS AVAILABILITY TEST.

a. **Objective.** This check is performed to verify that the American Power Conversion (APC) un-interruptible

power supply (UPS) units are connected and operating properly.

b. Discussion. After a period of time the batteries may fail to provide an adequate level of power in the event of a power shortage. The Built In Test (BIT) will verify that the batteries in the UPS units are fully charged and are able to provide adequate power to the workstations and file servers. If the UPS fails to switch to battery backup, then the unit should be replaced.

c. Test Equipment Required. None.

d. Conditions. None.

e. Detailed Procedure.

1) Press the button marked "TEST" located on the control panel and hold for 5 seconds. This invokes the BIT.

2) Verify that the UPS unit transitions to the battery backup by the "ON BATTERY" LED being illuminated.

3) Observe the "LOAD" LEDs to determine if the battery is fully charged. If the UPS fails to switch to battery backup or REPLACE BATTERY is illuminated, then the unit should be replaced.

6.2.2.14 ATCSCC COMMUNICATIONS CHECK

a. Objective. This check is performed in order to verify that the network is communicating to all user sites

b. Discussion. The ATCSCC has the capability to monitor and report on the status of all communication links to the user sites. The LINCS SSD Monitor has been established to record and display any communication warning or failure messages.

c. Test Equipment Required. None.

d. Conditions. The operator position must be on-line in the mode to display the LINCS SSD Monitor program information.

e. Detailed Procedure. On the LINCS SSD Monitor display, observe no communication failures are indicated.

6.2.2.15 TMU FILE SERVER TO HOST/ARTS COMMUNICATIONS CHECK.

a. Objective. This visual check is performed in order to verify that the Host or ARTS computer is communicating with the TMU File Server.

b. Discussion. The status of the TMU to the NAS HOST or ARTS computer interface is monitored by the Status Activity Monitor (SAM) unit. The SAM unit is physically located on the NAS computer to A/B Switch cable within two feet of the A/B Switch connected to the file server and the backup file server. In addition to the SAM unit LED status lights, the file server has the capability to monitor and report the status of communication by displaying a window, which scrolls the message traffic through the ETMS-ATC computer interface. The status window also displays a message counter and an error message if an interruption to the ATC NAS computer to TMU interface occurs. The window will display the message counts and other information in the following format:

Counts reset at: <date> <time>

TZ	CT REQ	CT SNT	AF	A Z	BZ	D Z	RZ	FZ	U Z
0	0	0	0	0	0	0	0	0	0

NAS is UP
DOWN.

Note: The last line on the status monitor window will be replaced with "The NAS is DOWN" message if the NAS ATC computer to TMU communication is inoperable.

c. **Test Equipment Required.** None.

d. **Conditions.** The TMU file server from which the check is being made must be on-line and be the active file server. The window status area display must be visible.

e. **Detailed Procedure.** Check for the LED light configuration and that the NAS is Up message is displayed on the active file server.

6.2.2.16 SPARE CISCO ROUTER SWITCHOVER CHECK.

a. **Objective.** To ensure the spare Cisco Router is available and is properly configured to provide fully functional backup capabilities and to serve as an adequate replacement for the primary router.

b. **Discussion.** The backup Router is provided to ensure the TMU has adequate redundancy for key system components. This change-out procedure is to verify the primary and backup Routers are capable of providing the same communication processing service for the TMU.

c. **Test Equipment Required.** None.

d. **Conditions.** None.

e. **Detailed Procedure.** TBD

6.2.2.17 SPARE CISCO ROUTER A/B SWITCHOVER CHECK.

a. **Objective.** To ensure the spare Cisco Router is available and is properly configured to provide fully functional backup capabilities and to serve as an adequate replacement for the primary Router.

b. **Discussion.** The backup Router is provided to ensure the TMU has adequate redundancy for key system components. The dual Router configuration provides a backup Router, available through the manual A/B switch. The procedure to test the backup Router has been established to verify the primary and backup Routers are capable of providing the same communication processing service for the TMU.

c. **Test Equipment Required.** None.

d. **Conditions.** None.

e. **Detailed Procedure.**

(1) Place the A/B switch for the Routers in the alternate switch setting to select the backup Router.

(2) On switchover, observe the statistics window on the file server has not lost communications with the TMCCC. The gate switch should a connection to another gate switch at the TMCCC.

6.3 NON-PERIODIC PERFORMANCE CHECKS

Non-periodic performance checks are performed only when it becomes obvious they are needed. A non-periodic performance check is usually heralded by some unforeseen or unanticipated event. The event is significant but does not

necessarily require corrective maintenance, per se. It simply requires an appropriate maintenance response (non-periodic maintenance).

6.3.1 Overview

Whereas periodic performance checks provide a periodic investigation into whether or not the system or a system component is performing properly, there exists another set of performance checks that need to be conducted only when there are indications that it may be worthwhile to do so. These are referred to as non-periodic performance checks.

6.3.2 Non-periodic Performance Checks Schedule

Since non-periodic performance checks are performed only when it becomes obvious they are needed, a formal schedule is not appropriate. In some cases a warning light may serve to focus attention. In other cases one or more abnormal error messages may warrant the non-periodic performance check. An example of such a performance check could be the error message that a printer paper jam has occurred. The paper jam turns out to be serious and the operations personnel feel that the situation requires a competent printer maintenance representative to correct the situation. The paper jam is serious and damage to the printer may result if the situation is not properly cared for.

A set of non-periodic Performance Checks are delineated in the table which appears on the following page. The set must be considered to be open-ended since it would be impossible to list all the possible candidate situations.

Table 6-2 Non-periodic Performance Checks

Performance Checks	*Maintenance Procedures*
AS REQUIRED **TMU operation** *(All sites)* (FAA Form 6110-9 Items)	
(1) Perform System Setup Procedures	**Error! Reference source not found.**
(2) Clean Tape Transport	6.3.3.2
(3) Remove Obsolete 56-day Update Files	**Error! Reference source not found.**
(3) Clean All CPU Tower Air Intake and Exhaust Vents	6.3.3.4
(4) Adjust Monitor Controls	**Error! Reference source not found.**
(5) Clean All Workstation Monitor Viewing Panels	6.3.3.6
(6) Clean All Computer Cabinet, Monitor Cabinet, Keyboard, Trackball, and Printer Housings.	**Error! Reference source not found.**

6.3.3 Non-periodic Performance Checks Detailed Procedures

The non-periodic detailed procedures are included in the following paragraphs.

6.3.3.1 PERFORM SYSTEM SETUP PROCEDURES

TBD

6.3.3.2 CLEAN TAPE TRANSPORT

a. Objective. The DDS tape format drive heads should be cleaned when the "Media Wear" (caution) light is displayed on the tape unit or after 25 hours of use. This procedure is also performed to verify that the 2 GB tape drive is connected and operating properly. Discussion. Tape drive, the "Media Wear" (caution) signal will be displayed when the unit requires cleaning. This "Media Wear" signal is displayed by LED1 flashing a green and amber light while LED2 is a steady green light. Errors in data transfer may be induced if this residue in not removed promptly.

b. Discussion. TBD

c. Test Equipment. Required. None.

d. Conditions. None.

e. Detailed Procedure.

(1) Load cleaning tape into the 2 GB tape drive per cleaning kit instructions.

(2) The tape drive unit will automatically clean the heads and eject the cleaning cassette at the end of the cleaning cycle.

(3) Remove cleaning tape when the process is completed. Write the current date on the label of the cleaning cassette to keep track of the cleaning date and the number of times the cleaning cassette has been used. Discard the cleaning cassette after 25 uses.

6.3.3.3 REMOVE OBSOLETE 56-DAY UPDATE FILES

TBD

6.3.3.4 CLEAN ALL CPU TOWER AIR INTAKE AND EXHAUST VENTS.

a. Objective. To provide maximum cooling to the internal components of the CPU.

b. Discussion. Modem LSI memory modules, cache memory and other high density packed CPUs are prone to premature component failure if the cooling air flow is disrupted. Dust, dirt, and carpet pile can block the air flow in the CPU. Periodic cleaning will ensure constant air flow to the CPU's internal components.

c. Test Equipment Required. None.

d. Conditions. None.

e. Detailed Procedure.

(1) Use a vacuum hose, preferably with a brush attachment.

(2) Clean the three grill openings on the rear of the CPU.

(3) Clean the grill area on the front of the CPU.

6.3.3.5 ADJUST MONITOR CONTROLS

TBD

6.3.3.6 CLEAN ALL WORKSTATION MONITOR VIEWING PANELS.

Clean the glass monitor panels by using a soft cloth or paper towel. Spray Windex or some other glass cleaning solution including water onto the glass surface and wipe clean.

Clean the front viewing panel of the high intensity monitors located in the control tower by using a water damp soft cloth. Do not use Windex or other cleaning solvents on the high intensity display panels.

6.3.3.7 CLEAN ALL COMPUTER CABINET, MONITOR CABINET, KEYBOARD< TRACKBALL, AND PRINTER HOUSINGS

TBD

6.3.3.8 HP TMCCC DATA REDUCTION.

a. Objective. This task is performed in order to provide data correlation and reduction for analysis of communication. It is intended to provide quality control tracking information of the wide area network communication for all user sites (ARTCCs, TRACONs, CERAPs, TMCCC, ATC

b. SCC, EOF, DOTS/EARTS/SCT/ REGIONAL OFFICES/HUGHES TECHNICAL CENTER/FAA ACADEMY).

c. Discussion. The TMCCC has the capability to monitor and report on the status of all communication links to the user sites.

d. Test Equipment Required. None.

e. Conditions. The operator monitor position must be on-line and in the mode to monitor and record network information.

f. Detailed Procedure. TBD.

7 TMU CORRECTIVE VERIFICATION MAINTENANCE

7.1 CORRECTIVE MAINTENANCE VERIFICATION PHILOSOPHY

From a corrective maintenance viewpoint, the underlying question, simply stated, is: From a usage viewpoint, can the operation of the system be relied upon? The goal of corrective maintenance verification is to first answer this question (at least to a reasonable degree of accuracy) and secondly, if the answer is no, to repair the system such that the answer to the question changes from no to yes.

As the concept of ETMS corrective maintenance verification matures, there will exist a set of corrective maintenance procedures which result in verification. These procedures, to be referred to as ETMS Corrective Maintenance Verification Procedures, will help answer the question as to whether or not corrective maintenance is required. They will, likewise, help answer the question the operability question after the repair has been accomplished.

7.2 TMU OPERABILITY ASSESSMENT

From time to time, the system user Traffic Management Specialist will report a system operability situation to the AF ETMS TMU maintenance staff on duty. It is the responsibility of the AF maintenance staff to determine if the reported situation is a result of a system problem or if nothing is wrong. If something is wrong, then it is the responsibility of the AF maintenance staff to correct the situation if it is within their on-site Level 1 capability and authority to do so. This includes obtaining Level 2 AOS-330 support, as may be required.

Some situations will be caused by hardware, some situations will be caused by software, and some may be caused by the manner in which the system has responded to some abnormal event which has occurred in the operational environment (anomalies). If the operational environment has produced such an anomaly, it may never happen again. An example of such an anomaly would be when, because of some external cause, an erroneous signal on a communication line causes the system to react in an abnormal way. Re-initialization may correct the problem and it is possible no one will ever know for sure, even after PTR analysis, the exact details, which surround the situation.

The vast majority of reported operational situations will be traceable, providing appropriate fault isolation techniques are used. Figure 7-1, Operability Assessment Tools, delineates tools the AF maintenance force have at their disposal on-site. These tools can help in the fault isolation process.

Paramount to the complete corrective maintenance process is the capturing of the system error state data via a memory dump. After the system error state data is captured through a memory dump in those situations which so warrant,, the corrective maintenance process can continue. After the problem has been corrected, the memory dump, if one has been taken, should be archived. for future reference. If a memory dump exists, it should be referenced in the Incident Report and/or the PTR, if a PTR is generated.

Figure 7-1 depicts the major operability assessment tools available to AF

maintenance personnel. Table 7-1 follows Figure 7-1 and elaborates the functionality of some of the more important existing operability assessment tools depicted in the Figure.

SUP MODE

SYSTEM
1. auto_message_display
2. backup_cartridge
3. backup_todays_files
4. buildup_all_nodes
5. buildup_node
6. certify_etms_software
7. cleanup_report_files
8. clear_baks
9. clear_current_files
10. clear_current_files_allnodes
11. clear_notify
12. clear_notify_allnodes
13. copy_to_network
14. delete_address_group
15. delete_log_data
16. delete_old_objects
17. delete_saved_msg
18. delete_std_message
19. delete_TSD_data
20. display_buffers
21. list_cartridge
22. reconfigure
23. remote_reboot
24. restart_processes
25. save_etms_dir
26. start_display
27. switch_fileserver

UNIX COMMANDS
1. ping
2. netstat
3. lanscan
4. lanadmin
5. landiag
6. dmon
7. top
8. tgs
9. ps
10. fsck
11. vmstat
12. chron
13. bdf
14. rlogin
15. lfconfig

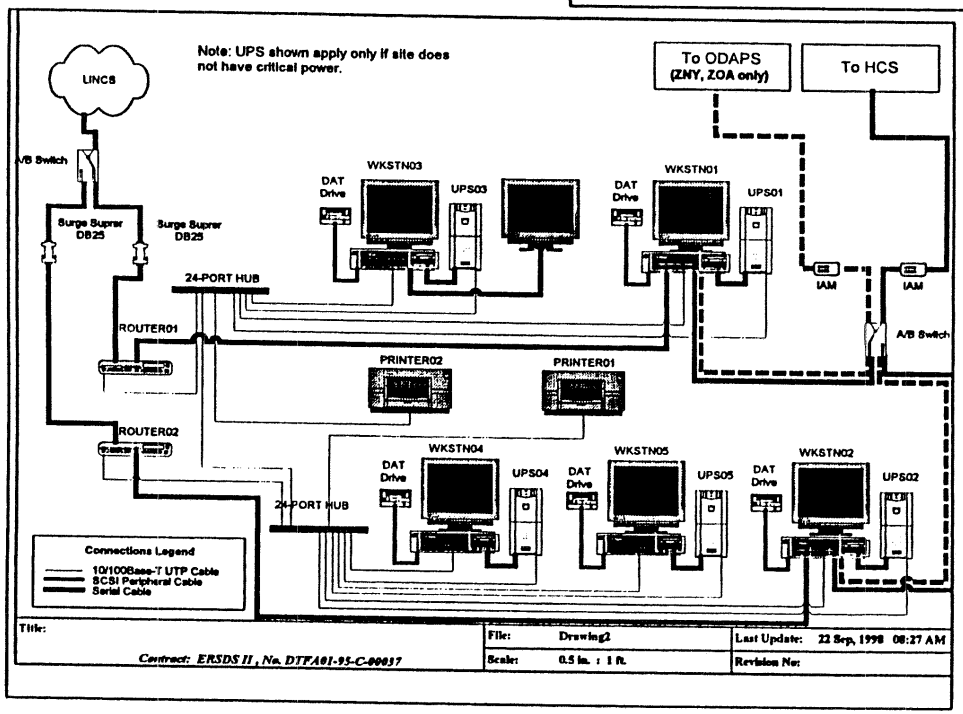
WATCHDOG

RESTORE
1. restore_cartridge
2. restore_from_win_disk
3. restore_todays_files

EDIT
1. edit_address_group
2. edit_advisory_prefix_to
3. edit_arinc_addresses
4. edit_arinc_src_code_to
5. edit_ATS_data
6. edit_etms_addresses
7. edit_groups_to_list
8. edit_icon_adaptation
9. edit_log_data
10. edit_message_footer
11. edit_nadin_addresses
12. edit_nadin_src_code_to
13. edit_print_flag
14. edit_rtr_adaptation
15. edit_saved_msg_file
16. edit_standard_messages
17. edit_sup_data
18. edit_TSD_data

MAINTENANCE
1. add_remove_a_printer
2. configure_rtr
3. list_etms_processes
4. list_hosts
5. list_logs → 1. Superuser Log, 2. System Log, 3. Shutdown Log, 4. RC Log
6. printer_admin
7. sam
8. select_printer_for_user
9. select_printer_for_ workstation
10. xstm

SYSTEM	DEVICE	TOOLS	OPTIONS
1. Select System to Test	1. Current Device Status	1. Information	1. Tool Options
2. Save Map	2. Clear Tool Status	2. Verify	2. Maps
3. Print Map	3. Select All	3. Diagnose	3. General
4. Remap System	4. Select Class	4. Exercise	
5. Map Log	5. Unselect All	5. Firmware Update	
6. License	6. Unselect Class	6. Expert Tool	
7. System Activity Log		7. Utility	
8. Daemons		8. Latest Logs	
		9. Tool Management	



1. Accounts for Users and Groups
2. Auditing and Security
3. Backup and Recovery
4. Clusters
5. Disks and File Systems
6. Display
7. Kernel Configuration
8. Networking and Communications
9. Performance Monitors
10. Peripheral Devices
11. Printers and Plotters
12. Process Management
13. Routine Tasks
14. Run SAM on Remote Systems
15. Software Management
16. Time

Figure 7-1 Operability Assessment Tools

Table 7-1 Operability Assessment Tools Functionality

Operability Assessment Tool	Functionality
Equipment LEDS Router Hub UPS DCU Tape Unit Printer	The system components contain a number of LEDs that indicate equipment status. These LED indications can be used in the troubleshooting process. Specific Led status information is contained in the respective individual system component Corrective Maintenance sections.
UNIX Commands	Detailed information on a UNIX command can be obtained by bringing up a window and typing man followed by cmd name Example: man ping | lp will print the ping command specifications.
ping----------	Ping sends ICMP Echo Request packets to network host or "box". Packets are sent once per second. Each packet that is echoed back via the ICMP Echo Response packet is written to the standard output, including round-trip time. Boxes that can be pinged include workstation, file server, hub, and router.
lanscan----------	Lanscan displays the following information about each LAN device that has software support on the system: Hardware path Active station address (Physical address) Card instance # Hardware state Network interface "Name unit" and state Network management ID MAC type HP DLPI supported (Indicates whether or not the LAN device driver will work with HP's Data Link Provider interface) Major number associated with the driver for the LAN interface. A - implies that a major # does not apply to this LAN device
rlogin----------	Rlogin connects your terminal on the local host to the remote host (rhost). Rlogin acts as a virtual terminal to the remote system. The host

Operability Assessment Tool	Functionality
	name rhost can be either the official name or an alias as listed in the file /etc/hosts.
telnet	Telnet is used to communicate with another host using the TELNET protocol. If telnet is invoked without arguments, it enters command mode, indicated by its prompt (telnet>). In this mode it accepts and executes a series of telnet type commands. Once a port has been opened on the named host. During the session, commands can then be entered for the remote host to execute
netstat	Netstat displays statistics for network interfaces and protocols, as well as the contents of various network-related data structures. The output format varies according to the options selected.
lanadmin	The landadmin program administers and test the LAN. For each interface card, it allows you to: Display and change the station address Display and change the maximum transmission unit (MTU) Display and change the speed setting Clear the network statistics registers to zero Display the interface statistics Reset the interface card, thus executing the self test For operations other than Display, you must have superuser privileges.
landiag	Refer to lanadmin
kermit	Kermit is a family of file transfer, management, and communication programs (Columbia University). Kermit for HP UX supports both serial connections (direct or dialed) and TCP/IP connections. Kermit is used to gain access into the router.
Ifconfig	Ifconfig allows a user to display the current configuration for an interface and also a user with the appropriate privileges to modify the

Operability Assessment Tool	Functionality
	configuration of a network interface.
Ioscan- -	Ioscan scans the system hardware, usable I/O system devices, or kernel I/O system data structures as appropriate, and lists the results. For each hardware module on the system, ioscan displays by default the hardware path to the hardware module, the class of the hardware module, and a brief description. By default ioscan scans the system and lists all reportable hardware found. The types of hardware reported include processors, memory, interface cards and I/O devices.
ps -	Ps prints information about selected processes. Use options to specify which processes to select and what information to print about them.
top ————————————————	Top displays the top processes on the system and periodically updates the information. Raw CPU percentage is used to rank the processes.
Examine Error Logs	
PowerChute	
Sup Mode -	The SUP Mode contains many sub-modes, some of which are relevant to corrective maintenance. Some but not all of the SUP modes appear in this table.
System -	
Certify ETMS Software - - - - - - - - - - - - - -	Compares the application and data files against a previously saved version. The dynamically changing tactical data files are <u>not</u> checked.
Switch File Server - - - - - - - - - - - - - - - - -	Allows access to the automated procedure for switching the File Server.
Restore	
Restore Last NADIN ARINC Files	
Restore Today's Files	
Edit	

Operability Assessment Tool	Functionality
Maintenance	
Add Remove A Printer - - - - - - - - - - -	Presents a screen menu to 1) configure 2)diagnose 3) Administer (Printer) 4)Administer (JetAdmin) 5) Printer Status
Configure Rtr - - - - - - - - - - - - - - - - - -	Allows entrance to the router via kermit
List ETMS Processes - - - - - - - - - - - - - -	Lists the set of currently active ETMS processes
List Logs -	Allows either viewing or printing access to one of the 4 system logs.
Supervisor Log - - - - - - - - - - - - - - - - -	
System Log -	
Shutdown Log - - - - - - - - - - - - - - - - -	
RC Log -	
List Hosts (lshosts) - - - - - - - - - - - - - - -	Presents a list of the current known host computers
Printer Admin - - - - - - - - - - - - - - - - - -	Allows selection of the Print Manager for the desired printer. Print Manager will show the printing queue status.
Sam -	System Administration Manager (SAM) contains features and functionalities that lend themselves to the troubleshooting process. SAM is part of the HP basic system. Consult the commercial documentation for SAM information. Root access is required to access the System Administration Manager.
Auditing and Security	
Audited Events	
Audited System Calls	
Audited Users	
System Security Policies	
Backup and Recovery	
Automated Backups	
Interactive Backup and Recovery	
Clusters	
NFS Cluster Configuration	
Disks and File Systems	
Disk Devices	
File Systems	
Logical Volumes	
Swap	

Operability Assessment Tool	Functionality
Volume Groups Display Monitor Configuration Xserver configuration Kernel Configuration Configuration Parameters Devices Dump Devices Subsystems Networking and Communications Bootable Devices DNS (Bind) Internet Access Name Service Switch Network Information Service Network Interface Cards Network Services Networked Site Systems System Access Performance Monitors Disk and terminal activity Inter-Process Communication Facility Process Processes with Highest PU Usage System Activity System Properties Virtual Memory Activity Peripheral Devices Cards Device List Disks and File Systems Monitor Configurations Plotters and Printers Tape Drives Terminals and Modems Printers and Plotters HP Distributed Print Service LP Spooler Process Management Process Control Scheduled Chron Jobs Routine Tasks Backup and Recovery Find and Remove Unused File sets Selective File Removal	

Operability Assessment Tool	Functionality
System Log Files System Shutdown Run SAM on Remote Systems Software Management Copy Software to Depot Install Software to Local Host List Software Remove Software Time NTP Broadcasting NTP Network Time Sources System Clock Xstm -	Xstm invokes the Support Tool Manager (STM). STM is part of the HP basic system. For detailed STM information, refer to the HP commercial documentation. STM provides a capability for managing the system and its devices.
System - Select System to Test Save Map Print Map Remap System Map Log License System Activity Log Daemons Device Current Device Status Clear Tool Status Select All Select Class Unselect All Unselect Class Tools Information Verify Diagnose Exercise Expert Too; Utility	Presents a graphic display of all the computer system components. Selection of a component runs an algorithm which then displays a status log for the selected device. **UPDATE IN PROGRESS**

Operability Assessment Tool	Functionality
Latest Logs Tool Management Options Tool Options Maps General	
Watchdog	Watchdog is a software package that is run at the Command Center and provides information about ETMS network performance.

7.3 TMU CORRECTIVE MAINTENANCE APPROACH

7.3.1 General Corrective Maintenance Approach

After a situation has been reported to the on-site AF maintenance staff, it is the responsibility of AF to correct the situation. Once AF verifies the situation, correction techniques may include repair or possibly interim "work around" procedures. The development of temporary "work around' procedures, if they entail an operational impact, must be coordinated with the Traffic Management Specialist. Permanent "work around" procedural implementation does not rest with field personnel.

After the corrective maintenance activity has been completed, AF should return an operable system for use by the Traffic Management Specialist(s). This is also true of a system component, which has been removed from the online configuration and is now being returned for online usage or standby status.

It is paramount that each TMU situation requiring corrective maintenance attention be entered into a log of on-going ETMS activities. This record not only provides a profile of overall TMU incidents, but it also provides a record of equipment change-outs etc.

The paragraphs which follow delineate a general corrective maintenance approach for the detection, isolation, and repair of a faulty system component.

7.3.2 Software Failures (General)

The detection and isolation of software based failures make it necessary to capture the system state as close to the time and situation of failure occurrence as possible. AF ETMS Open Systems Maintenance Directive # 1 addresses memory dumps, incident reporting, and submission of related PTRs.

Situations may also arise that make it necessary to implement emergency fixes in the field. AOS-330 will normally be involved with emergency type fixes.

7.3.3 Hardware Failures (General)

Hardware failures may be "hard" or they may be intermittent. In the case of intermittent hardware, error logs may need to be analyzed. Hardware substitution may

also be used in demanding and difficult intermittent fault diagnosis situations.

7.3.4 Restoration (General)

The Restoration Process may entail a number of different disciplines before the problem finally gets fixed. The Restoration Process has not been completed until operational capability has been restored.

The verification of an operational capability during the restoration process is an AF responsibility. This is not to say the Traffic Management Specialist may not be called upon to assist in making a final determination as to whether or not the problem has been corrected.

7.3.5 Corrective Maintenance Log and the Logging of Operational Incidents

FAA Form 6030-1 Facility Maintenance Log (Manual) should be used to log all corrective maintenance activity. As the Maintenance Management System (MMS), the NAS Infrastructure Management System (NIMS), and the National Operations Control Center (NOCC), mature, automation systems will be used to effect the corrective maintenance log entries.

Any activity that is required to correct a verification deficiency in the TMU is to be classified as a corrective maintenance activity. Example: Weather display has a weather detail not being properly displayed. After some coordination with the Help Desk and indirectly with Volpe Hub personnel, the situation is corrected. No re-initialization is necessary. This incident is to be treated as a corrective maintenance activity on the local TMU Corrective Maintenance log.

Only through the diligent logging of all operational incidents requiring remedial activity, can the system trends be accurately accessed and managed. Without this source data, TMU reliability cannot be accurately established and improved. To the degree incidents are accurately logged, meaningful source data will have been provided to the maintenance program improvement effort. As the effectiveness of the maintenance program itself improves, everyone can take pride in a job well done.

7.3.6 Major TMU Components Fault Detection, Isolation, and Restoration

A most important initial step in the Fault Detection and Isolation Process is the capturing of system state information for PTR incorporation. After this has been accomplished, the AF maintenance staff may proceed with the Fault Detection and Isolation Process. The tools illustrated in Figure 7-1 may be used by the AF staff to assist in the process.

Given a software situation, re-initialization may solve the problem. Whatever the corrective maintenance procedure to fix a particular problem entails, the objective is to return a system or system component that is ready for online operational usage.

The paragraphs, which follow, address TMU corrective maintenance fault detection, isolation and restoration for the major TMU system components.

7.3.6.1 Wide Area Network (WAN) Phone Lines

The ETMS WAN includes the Volpe Hub Routers, the TMU Routers, and the interconnecting telephone company FTS 2000 and LINCS communication lines and equipment such as the Data Service Units (DSUs) . MCI is the LINCs/FTS 2000 contractor.

AF is not responsible for maintaining the telephone line ETMS component. If the telephone lines are not working, however, AF may find it necessary to detect and isolate a problem to inoperable telephone lines in order to have the problem corrected and restore TMU operability. The TMU

Router is addressed separately in the paragraphs following telephone lines

7.3.6.1.1 Phone Lines Fault Detection and Isolation

DSU LEDs: Carrier light green indicates the presence of a carrier. Without the presence of a carrier, no signals can be transmitted. Carrier failure is a telephone company problem.

Diagnostics: If a carrier is present, the ping command can be used to help diagnose the absence of a telephone line communication path. The capability to ping a router on the LAN taken in conjunction with the failure to be able to ping a remote "box" via the WAN can be a significant indicator.

Additional UNIX commands useful for troubleshooting a phone line connectivity problem include rlogin, netstat, host, lanscan, and ifconfig.

7.3.6.1.2 Phone Lines Restoration.

Problems related to phone line operability should be reported to the phone company. The phone company is responsible for restoration.

7.3.6.2 TMU Local WAN Router

The Router connects the TMU Local Area Network (LAN) to the Wide Area Network (WAN). A cable connects a port on the TMU Hub to the Router. The Router is a CISCO 1601 unit. The Router hands-off all messages received externally via the WAN to the TMU hub and all messages received from the TMU hub to the WAN. The Router uses TCP/IP. TMU tactical sites normally have a primary router and a standby router, both of which use the same virtual address. To switch routers, it is necessary to switch the A/B Switch unit.

The CISCO 1601 Router has internal configuration files, diagnostics, etc. Access to the Router from a workstation is done via the UNIX based kermit command.

AF is responsible to detect a faulty router, replace it, and verify the operability of the replacement unit.

7.3.6.2.1 TMU Router Fault Detection and Isolation

Front Panel LED Indications:

SYSTEM PWR	Green indicates both AC and DC power is correct. If this light is out and AC power is being applied via the AC power cable, the internal power supply has failed.
SYSTEM OK	Green indicates the Router is booted correctly. If this light is off, it means the Router software is not operational.
RDY LED	If this light is not lit, it means the Router is not correctly connected to the external modem or other DCE equipment.
LAN ACT	Green indicates data is being sent to or received from the LAN. If light is steady green, it means the Router is continuously transmitting. Replace the Router.
LAN COL	Amber indicates, when flashing, there are packet collisions on the LAN.
SER 0 CD	Green indicates the Router has an active connection on the serial port.
SER 0 ACT	Green indicates Router serial port is sending or receiving serial data.
WIC CD/B1	Green indicates serial WAN interface card has an active connection on the serial port.

WIC ACT/B2 Green indicates WAN interface card serial port is sending or receiving data.

Back Panel LED Indications:

Flash PC OK LED: If this light is off, the Flash PC card is not correctly installed.

RDY LED:

LNK LED: (10BASE-T port) light is not lit. If router is connected to the LAN via 10 BASE-T port, the connection to the LAN has failed.

AUI Port Light: If lit and the Router is connected to the LAN via a 10BASE-T port, replace the hub.

Diagnostics: Router diagnostics include:

Ping and netstat

Lanadmin

Router Power-up

The active router an be pinged, the standby router can be pinged, and the virtual address can be pinged.

A number of Router diagnostics are run when the unit is powered-up. To exercise these diagnostics, first switch the Router in question to the backup position using the A/B switch. Then turn the Router power switch off and then back on.

Use of System Error Logs:

If Router problems are suspected, the System Error Log may also be examined for Router type error messages.

The Router also has an internal log file that can also be a source of diagnostic information.

7.3.6.2.2 TMU Router Restoration

Replace a Router found to be defective by making sure the Router is in the A/B Switch Standby Router status, turn-off the AC power switch, mark all cables to make sure they are properly reconnected, disconnect all cables from the defective unit, remove the defective unit, replace, reconnect all cables, turn on the AC power switch. Verify the operability by switching the router to the active on-line position.

7.3.6.3 TMU LAN Communications Hub

The TMU Hub is the central connection device for devices connected to the LAN. Each unit connected to the LAN does so via a cable, which is plugged into the Hub unit. These areas of Hub connectivity are known as ports. An autosensing Hub port has the capability to automatically detect whether the circuit is a 10 MBPS or a 100 MBPS data transfer connection. An up-link port is a port used to add a second Hub to the TMU configuration. This up-link port connects the two ports together and both Hubs then have interface ports for the TMU LAN devices. A Hub may contain 12 or 24 10 Base T/100 Base TX autosensing ports.

AF is responsible for detecting a faulty Hub, replacing it, and verifying the operability of the replacement unit.

7.3.6.3.1 TMU Hub Fault Detection and Isolation

LED indications are:

System Status LED - Green indicates the hub is functioning correctly.

Port LED - Rapidly alternating between green and amber indicates packet transmission is not correct. Check device at other end of port cable. Successful packet transmission causes the port LED to turn green.

Port LED - Solid amber indicates device at the other end of the port cable is not functioning correctly or the port is auto-partitioned

Hub diagnostics tools include:

ping

Netstat

Lanadmin

7.3.6.3.2 TMU Hub Replacement

HUB Replacement - First turn-off Hub AC power switch, then systematically remove all cables from the defective hub, making sure all cables are marked so they will be properly reconnected to the correct ports. Remove the defective hub, reconnect all cables, turn-on the AC power switch, and verify all hub LED indicators are providing the correct indications.

AF is responsible to detect a faulty hub, replace it, and verify the operability of the replacement unit.

7.3.6.4 Local Area Network (LAN) Hub Communication Interfaces

The ETMS TMU LAN utilizes an Ethernet architecture to interconnect the TMU Hub(s) with the workstations, file servers, printers, and the UPS units.

Tape drives, keyboards, trackballs, and internal disk units are not interconnected via the LAN, but interface directly to the computer with which they are used. The TMU Ethernet includes both 10 baseT and 100 baseT capabilities. 10 baseT transfers data at 10 MBPS and 100 baseT transfers data at 100 MBPS. The TMU hub automatically senses and adjusts to the different speeds. The LAN also includes all of the interconnecting cables and their connectors. Each device contains an Ethernet module which is designed to operate on the basis of Carrier Sense Multiple Access/Collision Detection (CSMA/CD) data transfer principle. Since all LAN devices interface directly with the hub, the topology is that of a star.

7.3.6.4.1 LAN Interconnection Fault Detection and Isolation

The LAN Hub device(s) are interconnected via cables and their connectors to the workstations, files servers, and UPS system components. Each of these devices contains an Ethernet interface card. In the case of the digital computers, AF maintenance personnel are prohibited from opening the cabinets to do such fault isolation activities as substitute a different Ethernet card. Since fault isolation is to be only to the cabinet level, After the Ethernet card becomes a suspect candidate, HP may need to be contacted.

The cables and their connectors should not normally fail while they are in service. If a failure occurs in the hub at the cable interface electronics, then the complete hub device is to be replaced.

Pinging to various units and from various units can be a principle fault isolation technique. It may also prove beneficial to disconnect a LAN device to determine if the rest of the LAN system components are functioning correctly when the unit is disconnected

7.3.6.4.2 LAN Restoration

Once the source of the faulty LAN communications interface has been determined, the failed unit should be replaced at the replacement unit level.

7.3.6.5 File Server

The file server performs several basic TMU functions. First, it acts as a common flight data repository. Second, it acts as a data source for those workstations using the Delay Manager. Third, the file server acts as the query device for forwarding data and report requests to the Volpe hub that have been generated via the workstations. Likewise it receives those query results from the Volpe hub back and forwards them to the requesting workstation.

While the workstation, working in conjunction with the monitor and other peripheral devices, provides a user type interface to the ETMS, the file server provides server type services to the workstations (clients). The file server is a significantly different concept than that of the workstation. The file server and the backup file server each share a cpu with a workstation.

The backup file server can be switched to online status. If a problem occurs in the file server, it is much more likely to affect all the online workstations configured in that specific TMU.

Since all cpu "boxes" have identical software configurations, the thing to do if a file server is suspect is to take that cpu off line, which will also take the workstation off line. If the workstation is in operational use, try to have the traffic management specialist move to a different workstation so the defective file server can be diagnosed. If this is not feasible, the diagnosis of the failed file server will have to wait until the workstation can be taken off line. Additional contamination of the system may result if an attempt is made to fault diagnose the unit on line. The secondary file server will be active online. The assumption is being made here that it will be safe to operate for a period of time with no backup. If this is not operationally acceptable, then a copy of the file server in another cpu configuration must be made the secondary file server.

Once the defective file server is off line, the corrective maintenance activity can begin. Once the dumps have been taken, reinitializing the system may solve the problem. If not, investigation must continue. Once the file server cpu configuration is taken off line, the LAN tools such as ping will not be available.

7.3.6.5.1 File Server Fault Detection and Isolation

The HP Support Tools Manager (STM) can be used to detect and isolate problems in the file server.

The file server system error log may also contain information that will prove useful in the detection and diagnosis of file server hardware and software components.

Depending on the symptoms, a number of UNIX commands and other tools illustrated in Figure 7-1 can be brought to bear on the problem. Additional UNIX commands useful for File Server and Workstation troubleshooting include start_utils, grep, sulog, rc.log, xstm, ioscan, fsck, bdf, dmon, top, kill, ps, vmstat, tar,, and shutdown. If reinitializing the system corrects the problem, as it should in many situations, an insight into what went wrong may have to await the PTR failure analysis process. Site personnel should always ensure an entry is made in the system log for each and every file server incident.

If the HP UX operating system or the digital computer hardware becomes suspect, collaboration with HP should take place. Opening of the HP digital computer will negate the computer warranty.

7.3.6.5.2 File Server Restoration

After the memory dump has been taken and the problem file server is no longer primary and the unit is off line, an investigation into what went wrong can be made. Once an investigation into the system state has been made, the first order of business should be to re-initialize the system. If re-initialization corrects the problem, then a return to normal operation is in order. If the backup file server hardware box must be replaced, that becomes an HP responsibility.

7.3.6.6 Workstation

The workstation is a digital computer with internal memories, an internal disk drive, a connected trackball, a connected keyboard, a connected tape drive, and a connected monitor. This specific area addresses only the digital computer internals. It does not address externally interfaced devices. The Monitor section includes the detection and correction of a defective monitor. The Monitor becomes the principle indicator that the digital computer is operable.

The workstation includes the HP UNIX based UX network operating system. The HP UX contains a number of commands that can prove useful in both establishing operability of the workstation as well as fault detection and isolation.

In addition to the operating system programs and data files, the workstation includes substantial amount of application software. This too can become the source of abnormal operation.

The workstation also contains an elaborate set of HP internal diagnostics, which can be used to detect and isolate problems.

The source of a software problem may be in either HP software or ETMS application software. These types of problems are normally referred to as software bugs. The first step to be taken when any abnormal workstation problem is detected is a scripted memory dump. If the system crashed, a memory dump is normally automatically taken and there is no need for a scripted memory dump. The memory dump should be taken to a reliable storage media, given the circumstance. This may be either internal disk storage or external magnetic tape, depending on the circumstance. PTR generation should normally follow the restoration of operability.

The ETMS workstation contains an extensive amount of application functionality. The ETMS workstation has many modes and many more sub-modes. A problem could possibly occur at any place at any time. While, in a reasonable number of cases, re-initialization of the workstation may well make the problem disappear, the PTR process is the only way to improve reliability. There are some 80 remote sites and as the replacement TMU installations progress, it becomes paramount to have each problem adequately documented and reported.

Problems should be expected and system stability and reliability cannot otherwise be achieved. The cost of not doing so becomes astronomical.

More than a single workstation may be affected. The WAN, and LAN common denominators are addressed under those respective topics. It should be understood and kept in mind that everything works together as a system, and that it is possible for a single point of failure to propagate with far reaching network implications. Taken in the aggregate, ETMS is a very large, widely distributed system and no single TMU is an island unto itself.

7.3.6.6.1 Workstation Fault Detection and Isolation

The vast majority of workstation based malfunction symptoms will first become obvious via the computer-human interface (CHI). Either the display will manifest abnormal symptoms or the response to input will be improper in some way. Again, before anything else is done, a memory dump should be taken, if the situation so warrants.. The memory dump captures the system state for use in possible later incident and/or PTR analysis.

How the fault detection and isolation process should proceed is very much a function of each individual problem situation. If the problem is software, system re-initialization may well correct a significant percentage of the situations. The situation wherein a single workstation is

malfunctioning, while other workstations are unaffected and available for operational usage, is obviously different from those situations wherein more than one workstation is being affected. If the weather across the United States is all clear and the ETMS is not being heavily relied upon for Traffic Management and flow control, the situation is different from the situation wherein an airport forecasted capacity has been reduced by 50% due to bad weather and the TMU is being relied upon for significant schedule modifications. The cost to an airlines for canceling a heavily booked flight into a reduced capacity airport is substantial, not to mention passenger inconvenience.

The main idea underlying work station fault detection and isolation is to not necessarily understand all the details of what has gone wrong, but to restore the operability of the system. If the system is needed for immediate usage, error analysis can take place after the fact based on the generation of a Incident Report and possible PTR. Depending on the nature of the malfunction, the longer a malfunctioning workstation is left online and the more things are done to the workstation, the more the possibility for contamination external to the workstation. Each situation is an individual call.

The quickest way to find out if re-initialization is going to solve the problem is to turn the power off and then restart the system. If the problem goes away and does not reappear, re-initialization after the memory dump is all that is required from an immediate on-site restoration viewpoint.

If the re-initialization does not correct the problem or if it reoccurs, then the failure isolation process must continue.

Whether or not additional corrective maintenance work needs to be done is obviously a function of the symptoms. Figure 7-1 maps a multitude of tools that can be used by the AF field maintenance force. The tools should be thoroughly understood through a comprehensive self-familiarization program. It should also be kept in mind the tools may not be functional, depending on the nature of the problem situation. An intermittent software bug that causes problems only when certain situations exists may require external software diagnosis support.

Defective hardware may be isolated via the HP UX STM hardware diagnostics. HP is available for suspected hardware related problems.

The Error Logs may also be used in the fault isolation process.

Intermittent problems pose a special fault isolation problem. Intermittent problems may, by their very nature, be unpredictable as to the frequency or conditions of their occurrence. One of the primary weapons to be used against the intermittent is the memory dump, especially if it can be taken while the system state still exists. Hardware can be a source of intermittence and isolation techniques may include module component substitution. Remember that opening the computer cabinet invalidates the warranty. The HP vendor should therefore be included in the isolation of intermittent hardware failures.

Maintaining operations log entries for all abnormal operating situations can prove helpful in solving intermittent type problems. If one and only one computer is doing it and the log substantiates this, a case can possibly be made against a single computer.

HP has a vendor warranty responsibility for the workstation basic hardware and operating system. HP should be contacted for assistance if symptoms point to the possibility of basic system problems.

7.3.6.6.2 Workstation Restoration

Reinitialized should be the first attempt at restoration. If this is successful, the incident should be logged and a related PTR should be generated.

If re-initialization does not result in the restoration of operability, then more diagnostic work should be done. Depending on the nature of the problem, it may not be desirable to replace the digital computer before having collaborated with HP.

7.3.6.7 Monitor

The Monitor provides the CHI display for the ETMS. As such, the Monitor is virtually integral to the digital computer from a human interface viewpoint. Fortunately, when Monitors fail or deteriorate, it is usually quite apparent they have done so.

7.3.6.7.1 Monitor Fault Detection and Isolation

If someone happens to be sitting in front of the Monitor when it fails, some form of abnormal screen transient will most likely be noticed. The transient may be in the form of a flash of light, pulsating intensity patterns, bands of light, etc. The extreme case will be a completely dead screen.

Any attempt to turn the Monitor off and then back on will more than likely either be completely unsuccessful or will result in a reoccurrence of the failure symptoms after a brief period of operation. The CRT high voltage internal supply is the Monitor component which usually deteriorates or fails.

When a Monitor failure occurs, the obvious thing to do is to turn the system off and then back on. If the failure persists, the Monitor power button should be turned off and the cables checked. If nothing is found to be wrong with the cables, then the unit should be disconnected and replaced. Turning on the replacement Monitor will quickly confirm the failed Monitor diagnosis.

7.3.6.7.2 Monitor Restoration.

After the failed Monitor has been removed and the new Monitor cabled to the AC power source and to the computer cabinet, turning on, the replacement unit more than likely will result in the restoration of operability. If the replacement monitor fails to function correctly, the Monitor drivers should be checked and the fault diagnosis continued.

7.3.6.8 Keyboard

The keyboard is an input device connected directly to the digital computer via an interconnecting cable between the keyboard device and the rear of the computer. The keyboard is not part of the LAN.

AF is responsible for fault detection and isolation. The Vendor is responsible for replacement.

7.3.6.8.1 Keyboard Fault Detection and Isolation

There are two principle techniques for detecting and isolating errors related to the keyboard. The first is by direct observation of how the system responds to input from the device. If a specific key is depressed on the keyboard and an improper input response is generated on the screen or if, the depression of a key does not "feel right", then there may be a defective keyboard.

Keyboard substitution is relatively easy. Either a spare unit or a keyboard device borrowed from another TMU computer may be substituted for the questionable keyboard. While it is permissible to remove and reconnect a keyboard without down sequencing the computer, doing so will deprive the maintenance person of the benefits of diagnostics that are run when the computer is up-sequenced. If the replacement keyboard works correctly and if the keyboard in question, when plugged

into another digital computer malfunctions in that other configuration, the keyboard may be assumed to be defective.

A second diagnosis technique is to simply power down the computer that has the keyboard in question and then power the computer back up. When the computer is powered up, the Power-On Self-Test (POST) automatically performs a series of tests that check the primary configuration components. If the POST detects a serious error in the keyboard, the boot will be halted and an error message generated. Such errors are sometimes included in the fatal error category. Keyboard error codes may be numbered in the 300 range. An 06XX code could also indicate a keyboard error.

Keyboard error codes include:

301	stuck key (XX 301,XX=scan code in hex
302	System unit keylock switch is locked
303	Keyboard controller failure
304	Keyboard clock high
305	Fuse on motherboard blown
341	Keyboard error
342	Keyboard cable error
343	Keyboard LED or cable failure
352	Keyboard not responding to POST test
353	Keyboard not responding to POST test
354	Keyboard self-test failure
365	Keyboard LED or cable failure
366	Keyboard interface cable failure
367	Keyboard LED or cable failure
370	Keyboard
371	Keyboard
372	Keyboard
06XX	Keyboard stuck key failure; XX=Scan code (hex) of the key

7.3.6.8.2 Keyboard Restoration

Power down the digital computer, remove the keyboard cable from the rear of the computer, replace the defective keyboard with an operable unit, and power up the digital computer. This will ensure any internal error situations caused by the defective keyboard are removed from the system.

7.3.6.9 Trackball

The trackball is connected to the digital computer via a cable that plugs into a jack located on the rear panel of the digital computer. The trackball is not connected to the LAN.

AF is responsible for trackball fault detection, isolation, and restoration.

7.3.6.9.1 Fault Detection and Isolation

The most common symptom of a trackball problem will be the failure of the cursor to respond when the trackball is moved. This failure to respond includes the situation wherein the cursor moves only sometimes and then it may be only in a jerky and partial response.

This jerky response is usually indicative that the trackball needs to be cleaned. Dirt and film have a tendency to accumulate on the trackball itself and also on the pick-off devices that sense the trackball vertical and horizontal motion.

7.3.6.9.2 Trackball Restoration

If trackball response is jerky, dismantle the trackball and clean the contaminated areas

with a commercial 70% rubbing alcohol solution

If there is no cursor response to the trackball whatsoever, power down the digital computer to which the trackball is connected and reinitialize the system. A software problem may have originated and the internal task management system may not be able to execute the task which responds to trackball movement. This will in essence, lockout the user.

If, after system re-initialization, the cursor still fails to respond to trackball movement, check for the presence of the trackball driver. The device driver can be reloaded to eliminate this software as a potential problem source.

If the preceding restoration procedures do not correct the problem, power down the digital computer, remove the trackball cable from the rear panel of the digital computer, replace the trackball, and restore power. If the cursor now responds, the trackball unit is defective. If the replacement trackball makes no difference, continue with the diagnosis.

7.3.6.10 Tape Station

The TMU tape drive is an HP Digital Data Storage - (DDS-3) type drive. It has a capacity of 12 Gigabytes under normal usage and a 24-Gigabyte capacity if data compression is used. Because of their removable storage media, magnetic tape devices can be used to provide backup data storage for operational systems. They are also used to store numerous types of files. The load tapes are used to store the operational programs and data for system initialization. The memory dumps used to support Problem Trouble Reports (PTRs) and Incident Reports, can also be stored on magnetic tape media.

The tape device is connected to the digital computer SCSI data bus and is not connected to the LAN.

7.3.6.10.1 Tape Device Fault Detection and Isolation

LED Indicators

STATUS	LEFT LED	RIGHT LED
No Power	Off	Off
Cartridge loaded, no R/W activity	On	Off
Cartridge loaded, R/W Activity	Flash	Off
Loading. Unloading Ejecting	Pulse	Off
Self Test Fail	Off	On
No cartridge, Caution (cleaning required)	Off	Pulse
Cartridge loaded, Caution (cleaning required)	On	Pulse
STATUS	LEFT LED	RIGHT LED
Cartridge loaded, Drive Active, Caution (cleaning required)	Flash	Pulse
Cartridge loading/ Unloading, Caution (Cleaning Required)	Pulse	Pulse

Note: Flash rate = 4 Hz
Pulse rate = 2 Hz

Diagnostics

The UNIX command ioscan can be used to obtain a device profile, which should include the tape station.

Enter /usr/sbin/ioscan -d stape

System should return tape drive details. If message "ioscan: No hardware found" is returned, a problem exists and continue with diagnostics.

Verify Device Drivers by:

Select SAM>Peripheral Devices

Double click on tape drives

Click on Desired Tape Drive

Then Actions>Show Device Files

Device files are listed with an explanation of each one. If no device files are listed, restore the device driver.

Checking the error logs and powering up/down the external DAT drive are also viable diagnostic activities.

7.3.6.10.2 Tape Station Restoration

If a defective tape station is found, HP is responsible for removal, replacement, test, and repair support.

7.3.6.11 Printer

The HP Deskjet 1600 CM is a color printer. Four separate ink cartridges provide the ink for color printing. One contains black ink and cartridge each for red, green, and blue ink. Only the black ink is required if no color is to be printed. The 1600 can print 8 ½ by 11 letter size paper, legal size paper, labels and envelopes. The 1600 cannot print 11 by 17 inch paper size. The 1600 can print in either portrait or landscape. Landscape is the name given to the letter paper size page that is printed with the 11 inch side of the paper across the top. The 1600 Printer can also be used to print transparencies.

When one of the ink cartridges runs out of ink, a light comes on the printer and an error message is generated in response to the print command.

Detecting a problem with the printer is usually not difficult. Either an error message will appear on the screen in response to a printer related command or there will obviously be something wrong with the way the printer is responding or with the printed page produced by the printer.

The printer is a device connected to the LAN and has a built-in Ethernet card.

AF is responsible for fault detection, isolation and printer replacement.

7.3.6.11.1 Printer Fault Detection and Isolation

LED Indicators:

Ready Light Flashing: Flashing Ready light indicates the printer requires attention.

Form Feed Light is on: Form Feed light indicates the printer is tying to use the Manual Feed Tray. Use of the Manual Feed Tray is controlled by the Printer Setup window.

Check Paper Light On or Flashing: Light signals a problem exists with the paper feed.

Check Print Cartridge normally indicates the cartridge has run out of ink and requires replacement before the printer will print.

Printer Diagnostics:

If difficulties are encountered in response to Print Commands, error message windows may appear on the Monitor. An inspection of the printer will normally indicate what action is required.

Printer diagnostics are available to check out the printer. Refer to the SUP mode.

7.3.6.11.2 Printer Replacement

HP is technically responsible for removal, replacement, test, and repair support in case a defective printer is found to exist in the configuration.

To replace the printer, power the printer down, disconnect both the LAN signal cable and the AC power cable from the rear of the printer, remove the printer, replace with an operable unit, reconnect the LAN signal and the AC power cables, and make sure the replacement printer contains a supply of paper and a complete set of ink cartridges. The ink cartridges may be removed from the printer being replaced and reinstalled in the replacement printer. Note: Printer ink cartridges cannot be removed and left lying around because once the seal is removed from the print head of a new cartridge, the

ink in the print head can dry out, clogging the tiny print nozzles. Turn the replacement printer on and run a self-test by pressing the printer front panel right-most button.

At the bottom of the printed self-test page labeled HP DeskJet 1600CM Self Test Page, locate the Interface Card Heading (bold type). Visually scan down the list to the 3rd entry labeled LAN HW ADDRESS: An entry example for the HW Address is 0060B0C97349.

Sequentially go to each computer that is to have the capability for usage of this printer and perform the following procedure:

1) Log in as root.
2) Click on the Personal Applications Icon and select Text Editor from the resulting window.
3) Select File>Open from the Text Editor Window.
4) In the Text Editor Open File window enter /etc for the Path entry and enter bootptab for the file name entry. Click on OK. The contents of the bootptab file will be on display
5) Use the down arrow to move the cursor down through the file contents to the line that indicates printerXX:\ where XX denotes printer #. If the system has more than one printer, be sure to locate the entry for the printer being replaced. At about the 5th line further down locate the ha= some entry and set this variable equal to the HW address previously located on the self-test printout..
6) Save the updated file and exit from the Text Editor window.
7) Select Terminal and in the resulting window command line type ps -ef | grep bootpd. If the bootpd process is running an entry such as root 990 743 0 Beb 16 ? 0:13 bootpd will result.
8) If the bootpd process is not running enter the command bootpd and repeat the verification.

After the bootpd files in all computers having access the replaced printer, power down the replacement printer and then power the printer back up. Print both a TSD snapshot (Tools>Snapshot) and a text file. Inspect the output for print quality.

7.3.6.12 File Server to NAS ATC Computer Interface

The TMU file server contains an EMULEX interface card which is used to provide an online interface to the local ARTCC Host computer, or to the local TRACON ARTS III-A computer, or to the EARTS OSC or CERAP computer. This local computer interface receives aircraft flight related messages from the ATC computers and in the case of the ARTCC, forwards the CT Message to the En Route system. (This CT message is the message that actually holds the aircraft on the ground until the capacity of the destination airport can accommodate the flight schedule.) This on site NAS ATC interface is not part of the ETMS TMU LAN, per se.

The ATC equipment complex is monitored by the ARTCC SMCC There is also an Inline Activity Monitor (IAM) used to monitor the interface. Also, note by referring to Figures 4.1 and 4.2 that there is an A/B switch located in this interface to the ATC computer. This A/B switch facilitates interconnection to either TMU file server.

7.3.6.12.1 NAS Interface Fault Detection and Isolation

IAM LEDs

LED # 2 Green: Red flash for data transmission

LED # 3 Green for continuity: Red flash for data transmission

If LEDs # 2,3,15,17 are green and no Red, then the NAS Driver is not running on the file server

If no Red LED on # 3, then the HOST computer is down. This seldom occurs.

Diagnostics

Check NAS driver by command ps -ef. NAS driver resource utilization: At prompt type dmon or top and verify the nas.driver is less than 5 %of the resources.

7.3.6.12.2 NAS Interface Restoration

If the NAS driver is not running, type restart_nas

7.3.6.13 Tower LAN Interface

Like the other TMU workstation and file server computers that are interconnected via the LAN, a control tower that is in close proximity to a TRACON TMU may also have a workstation interconnected to the TRACON TMU via the LAN. This interconnection may include a set of media converters that help span the distance by converting the signal to a reduced bandwidth requirement. This reduced bandpass (10Base 2) signal facilitates a longer cable. Refer to Figure 4-2 for configuration details.

Also, notice in Figure 4-2 there are two surge protectors located between the media converters. These surge protectors protect the lines against lightening and other voltage surges. These surge protectors are made of metal oxide varistors (MOVs) that clamp and shunt any voltage in excess of a threshold value. Surge protectors may have a status light, breaker fuse, or both.

The control tower workstation works as does any other TMU workstation with the exception the associated Monitor may have a brighter screen illumination capability to compensate for the daylight illumination that may exist in the control tower.

7.3.6.13.1 Control Tower Fault Detection and Isolation

Refer to the Workstation section for Workstation fault detection and isolation.

The surge protector light should normally be lit. If not lit, the surge protector MOV has blown. If the surge protector has a circuit breaker, reset. Otherwise, replace the surge protector.

Media Converters: **TBD**

Repeaters: **TBD.**

7.3.6.13.2 Control Tower Restoration

For Workstation Restoration, refer to the Workstation Restoration section.

For surge protectors, either reset the circuit breaker or replace the surge protector unit.

Media Converters: TBD

Repeaters: TBD

7.3.6.14 UPS

In addition to the prime power connectivities, the UPS is also connected as a LAN device. This allows LAN access to the internal UPS parameters, self-testing, etc.

The basic idea behind the UPS is that it contains a set of one or more batteries that remain charged under normal operating conditions. If the AC prime power should fail, an inverter internal to the UPS starts up (DC to AC converter) and picks up the AC load with no detrimental or visible load interruption occurring.

When AC prime power being supplied to electronic equipment is suddenly removed or interrupted because of a prime power failure, accidental throwing of circuit breakers etc., the reliability of the electronic equipment can be adversely affected. Depending on the nature of the failure, it is possible for severe transients to occur on the AC power line. Such prime power failures can induce a number of faults into the equipment being supplied by the prime power source. Some of these faults may appear immediately when prime power is returned. Others may take days, week, or months before a failure caused by a

"weakened" circuit finally materializes. The result can be a serious compromise to equipment reliability, not to mention the maintenance "nightmare" which can ensue. Because of this possible consequence to a prime power failure, it is prudent to have the UPS backup power systems ready to do their job at all times. No one can anticipate when the next prime power failure may occur. Years may go by or there may be a sequence of several in a matter of minutes.

The UPS units also correct for line voltage variations of both a slow variation and a surge nature. Spikes are also removed by the UPS units. These UPS capabilities can also improve equipment reliability because internal power supplies may not be able to otherwise provide the required DC voltage regulation under such circumstances.

The UPS internal battery may supply power for up to 16 minutes. The maximum load is 950 watts. The battery is sealed and has a normal life of from 3 to 6 years. Recharge time from a total discharge state may be from 2 to 6 hours.

If the quality of the AC Prime power is poor, the UPS may frequently transfer to battery based operations. The threshold for when a warning is provided for a low battery condition is adjustable. Audible beeps are provided for low battery conditions. The UPS contains automatic self-test functions which are exercised when the UPS is turned on as well as on a predefined adjustable type schedule. Front panel LEDs are used to indicate both high and low line voltages.

The TMU digital computers each contain software for monitoring and adjusting the UPS. This software package is referred to as PowerChute and can be invoked by typing PowerChute at the Command Line.

The UPS can be started using its own internal power if no AC prime power is available. The UPS automatically charges its internal battery system as long as it is in operation and is running off AC Prime Power.

The commercial documentation for the UPS and PowerChute in particular can provide additional information.

7.3.6.14.1 UPS Fault Detection and Isolation

LEDs:

Online LED: Illuminates when the UPS is providing prime power to the loads.

Site Wiring LED: Illuminates when thee is a site wiring problem

Replace Battery LED: Illuminates when a UPS self-test fails. Light is accompanied with a 1 minute audio beep and repeats every 5 hours

5-LED Display (right side): Indicates the percentage of battery charge. All illuminated indicates full charge. Top LED goes out when battery is less that 100%. When all LEDs are flashing, battery supply is less than the low battery warning interval time for the load.

Smart Trim LED: Indicates the UPS is compensating for high voltage

Smart Boost LED: Indicates the UPS is compensating for low voltage

Voltage Bar Graph (5 LEDs on Right Side) The 5 LEDs will indicate the input line voltage by pressing and holding the ON-TEST button. After 5 seconds the 5 LEDs indicate the line voltage. When 3 LEDs are illuminated, a line voltage between 115 and 123 Volts is indicated. No LEDs illuminated indicates a very low line voltage. All LEDs illuminated indicates a high line voltage

Configuration LED: UPS detects line voltage variations such as spikes, notches, dips and swells and distortions that may be caused by some prime power sources. UPS reacts by transferring to battery operations

to protect the loads. If it is permissible for loads to operate normally under these conditions, battery capacity and life can be preserved by reducing the sensitivity of the UPS to this automatic switchover. This sensitivity can be set using the Configuration button which works in conjunction with the Configuration LED. Use a pointed object , depress the button once to set the UPS sensitivity to a reduced value. This will cause the Configuration LED to become dimly lit. Depress again to set the sensitivity to the LOW setting. This will cause the Configuration LED to not light at all. Depressing the button a third time returns the UPS to the normal sensitivity setting. The Led will be illuminated brightly.

Back-panel Circuit Breaker: The UPS Back-panel circuit breaker trips if the load exceeds 950 watts. (Could have been caused by a temporary short circuit.) Depress the circuit breaker to reset.

Diagnostics:

Indications provided by the front panel LEDs can be used in the diagnostic process:

Front panel indicators flash sequentially: UPS has been shut down via remote control. UPS will restart automatically when Prime Power is again applied. This situation may possibly result from a scheduled shutdown to perform prime power maintenance activity.

All indicators are lit and the unit emits a constant beeping: This situation indicates an internal UPS fault. Do not attempt to use the UPS until the unit has been serviced.

All indicators are off and the UPS is plugged-in: The battery is discharged from an extended prime power outage. The UPS will automatically return to service when the prime power is reapplied and the battery has acquired a sufficient charge.

Replace Battery LED is illuminated: The batteries are weak. Allow for a four hour recharge. If the problem then persists, replace the batteries. If the Replace Battery LED remains lit after batteries have been replaced, the batteries may have been improperly installed.

5-LED Display LEDs are flashing: Battery voltage is less than the low battery warning time interval for the load.

PowerChute: PowerChute can be invoked by typing PowerChute at the Command Line. PowerChute includes a capability to monitor how the UPS is functioning.

Four menus facilitate access. They are:

The System Menu allows the monitoring of a different file server, to schedule server shutdown dates and times, or to shutdown the file server immediately and exit PowerChute

The Logging Menu allows the setting of logging options, view the event log, view the data log operating parameters, configure the UPS shutdown parameters, set communications parameters, configure flex events, flex event users, set Measure UPS parameters, and to tailor monitoring preferences

The Diagnostics Menu allows for testing of the UPS. Allows test scheduling, initiate self tests, initiate run time calibration, simulate a power failure, and initiate a UPS alarm test.

The Configuration Menu: allows the setting of UPS operating parameters, configure UPS shutdown parameters, set communication parameters, configure flex event and flex event users, set Measure UPS parameters, and tailor monitoring preferences.

The Hardware and Status Menus located in the Main screen in the upper left corner. This display shows:

The monitoring Host computer name
The UPS Model displays the model and number of the UPS

The UPS Status displays the current UPS operational status. The UPS Status contains different entries as a function of UPS malfunction, test in progress, or abnormal condition system states. This display contains critical fault diagnosis information.

7.3.6.14.2 UPS Restoration

Restoration activity will normally consist of allowing the batteries to recharge to a point where they can safely carry the load if they become completely discharged or replacement of the unit.

7.3.6.15 Surge Supressors

TBD

7.3.6.16 A/B Switches

TBD

7.3.6.17 Repeaters

TBD

7.3.6.18 Cables and Connectors

TBD

8 ABBREVIATIONS AND ACRONYMS

ACES	Adaptation Controlled Environmental System
AF	Airway Facilities or Flight Plan Amendment Message
AFB	Air Force Base
AFTN	Aeronautical Fixed Telecommunications Network
AIS	Aeronautical Information System
AOS	Operational Support (FAA organization)
APC	American Power Conversion
A/P	Airport
ARF	Airport Reservation Function
ARINC	Aeronautical Radio Incorporated
ARTCC	Air Route Traffic Control Center
ARTS III-A	Automated Radar Terminal System III-A
ARTS III-E	Automated Radar Terminal System III-Enhancement
AT	Air Traffic
ATC	Air Traffic Control
ATCSCC	David J. Hurley Air Traffic Control System Command Center
ATCT	Air Traffic Control Tower
ATO	Air Traffic Operations
ATR	Apollo Token Ring
AUI	Attachment Unit Interface
BIT	Built in Test
BO	Buffer Overload

CARF	Central Altitude Reservation Function
CCM	Communications Control Module
CDE	Common Desktop Environment
CERAP	Center Radar Approach Control
CDT	Controlled Departure Time
CFC	Central Flow Control
CFCC	Central Flow Computer Complex
CFCF	Central Flow Control Function
CHI	Computer-Human Interface
CM	Configuration Management
CMD	Command
COM	Communications
CPU	Central Processing Unit
CRON	UNIX Chronology Daemon
CSU/DSU	Channel Service Unit/Digital Service Unit
CT	Control Time Message
CVRS	Computerized Voice Reservation System
DAT	Digital Archive Tape
DB	Database
DDS	Digital Data Storage
DoD	Department of Defense
DOTS	Dynamic Oceanic Tracking System
DZ	Departure Message
EARTS	En Route Automated Radar Tracking System
EDCT	Estimated Departure Clearance Time
EOF	Emergency Operations Facility

ERL	Environmental Research Laboratory
Ethernet	IEEE 802.3 Network
ETMS	Enhanced Traffic Management System
FA	Fuel Advisory Delay Table or Message
FAA	Federal Aviation Administration
FAALC	FAA Logistics Center
FDB	Flight Database
FML	Facility Maintenance Log
FMS	Flow Management Specialist
FS	Scheduled Flight Message
FSS	Flight Service System
FT	Terminal Weather Forecast Message
FTM	Flight Table Manager
FTP	File Transfer Program
FTS 2000	Federal Telecommunications System
FZ	NAS Flight Plan Message
GA	General Aviation
GB	Gigabyte (10^9)
HCS	Host Computer System
HDTA	High Density Traffic Airport
Host	Host Computer System (ARTCC ATC)
HP	Hewlett Packard
IAM	Inline Activity Monitor
IBM	International Business Machines
ID	Identification
IFR	Instrument Flight Rules

IP	Internet Protocol
I/O	Input/Output
KB	Kilobyte (10^3)
KBPS	kilobytes per second
LAN	Local Area Network
LCD	Liquid Crystal Display
LINCS	Leased Interfacility NAS Communication System
MA	Monitor Alert
MB	Megabyte (10^6)
MGMT	Management
MSG	Message
NADIN	National Airspace Data Interchange Network
NAS	National Airspace System
NAVAID	Navigation Aid
NCP	NAS Change Proposal
NFDC	National Flight Data Center
NOAA	National Oceanographic and Atmospheric Administration
NOS	National Oceanic Service
NOTAM	Notice to Airmen
NSN	National Stock Number
OAG	Official Airline Guide
OCS	Offshore Computer System
ODAPS	Oceanic Display and Planning System
OFDPS	Offshore Flight Data Processing System
OS	Operating System
PAMRI	Peripheral Adapter Module Replacement

PM	Preventive Maintenance
PVD	Plan View Display
RMD	Resource Management Display
RMGR	Route Manager
RO	Receive Only
RS	Scheduled Flight Cancellation Message
RZ	Cancellation Message
SA	Surface Observation (weather) Message
SAX	System Exerciser
SCDT	Scheduled Controlled Departure Time
SCSI	Small Computer System Interface
SCT	Southern California TRACON
SDD	Software Design Document
SI	Substitute Processing Message
SID	Standard Instrument Departure
STAR	Standard Arrival Route
STARS	Standard Terminal Automation Replacement System
SUA	Special Use Airspace
SUP	Supervisory Mode
TBD	To Be Determined
TCP/IP	Transmission Control Protocol/Internet Protocol
TFMI	Traffic Flow Management Infrastructure
TM	Traffic Management
TMC	Traffic Management Coordinator
TMCCC	Traffic Management Central Computer Complex
TMS	Traffic Management System
TMSH	Traffic Management Shell

TMU	Traffic Management Unit
TO	Oceanic Position Update Message
TPR	Technical Performance Record
TRACON	Terminal Radar Approach Control
TSD	Traffic Situation Display
TWR	Tower
TX	Transmit
TZ	ARTCC Generated Message that Gives Aircraft Position and Time
UPS	Un-interruptible Power Supply
UZ	ARTCC Boundary Crossing Message
VFR	Visual Flight Rules
VNTSC	Volpe National Transportation Systems Center
WAN	Wide-Area Network
WC	Weather Coordinator
WJHTC	William J. Hughes Technical Center
WSI	Weather Services International

APPENDIX A. CAPABILITIES VERIFICATION REQUIREMENTS

Table A-0-1. TSD Capabilities Verification Requirements

Traffic Managtement Service	*Capabilities Verification*	*Performance Criteria*
DISPLAY:		
MAPS:		
FLIGHTS: TSD provides display of flights and flight counts. Groups of flights selected for display may be filtered. Specific flights may be found and supplemented with additional information		
ALERTS: TSD provides a capability to set and monitor traffic thresholds		
WEATHER: TSD provides weather	1. Weather Menu	Select Show Weather

Traffic Managtement Service	*Capabilities Verification*	*Performance Criteria*
information	2. Show/Hide Weather	
	2.1. Select Weather Sequentially select each of the following five sub-modes and check performance against the stated criteria	
	2.1.1. NOWRAD (2km)	NOWRAD (2km) resolution weather Radar is displayed for TSD geographical area . Click on Adapt and then sequentially select Level 1 to Level 6. Level 1 shows the least weather and Level 6 shows the most weather. The display should progress from Level 1 to Level 6. The 2 km is a higher resolution than the 8 km. Display is updated every 5 minutes.
	2.1.2. NOWRAD (8km)	Repeat for the 8 km display what was done for the 2 km display. Results should be similar. The 8 km is a lower resolution than the 2 km. Display is updated every 5 minutes.
	2.1.3. Radar Tops	Radar Tops displays the altitude of cloud tops within precipitation areas. First select the NOWRAD, then Radar Tops (If necessary, use the Adapt button to modify the default color of the cloud tops. Click on Apply or OK.) The TSD should be redrawn with the cloud tops appearing in the desired color. The Cloud Tops display should be updated every 10 minutes.
	2.1.4. Lightning	The lightning display presents a 1 hour accumulation of lightning strikes. A new update set is added every 5 minutes. Click on the Adapt button to obtain the Lightening History display. Clicking on the latest shows the most recent 5 minutes update. Each 5 minute interval of

Traffic Managtement Service	*Capabilities Verification*	*Performance Criteria*
		strikes can have a distinct color assigned. The lightening display should result in one or more clusters of + symbols (depending on the severity and locations of thunder storms), with each symbol representing a strike.
	2.1.5. Jet Stream	The jet stream is displayed as a series of contours depicting wind speeds of 70 knots or more. The different adjacent contours represent wind speeds differing by 20 miles per hour. Each contour depicts the wind speed in knots, the wind altitude, and the wind direction.
	2.1.6. Report	The Adapt box allows the selection and customization of three overlays Selection of Report results in a Command line window. Type WX airport to display a weather report for any given airport. Example WX phl.
REROUTE: TSD provides the capability for defining and managing suggested reroutes to assist pilots in the avoidance of severe weather. These alternate routes are displayed in graphic form.	3. Reroute Menu Show/Hide The Show capability displays a list of reroutes that are currently hidden from the main graphic display. Selection of one or more currently hidden reroutes will result in their graphic display. The Hide capability displays a list of currently displayed reroutes. Selection of one or more of these currently displayed reroutes will	Select Show/Hide

Traffic Managtement Service	*Capabilities Verification*	*Performance Criteria*
	result in their removal from the main graphic display.	
	Create Reroute	Select the Create Reroute sub-menu.
	The Create Reroute command provides for the definition and display of reroutes on the TSD.	For the name entry type Test. For the Reroute field type BOS.MHT.CAM.J547.BUF.ECK For the Void Time entry type current time + 5 minutes Click on the Name, NAVAIDs, Intersections, and Distance boxes Click on the Color Box and select a color. Click OK The Reroute should display as follows:
	Edit	Click on the Edit sub-mode menu.
	The Edit command provides for editing a reroute	Click on the Test reroute from the display of reroutes currently defined. Click on the OK box.
	Delete	The Edit display window is the same as the Create Reroute display window
	Send	
	Import	Deselect the Name, NAVAIDs, Intersections and Distance boxes.
	Show ATCSCC Reroutes	Change the Reroute entry from XXX to YYY. Click OK. The Reroute should display as follows:.
	Delete	Click on the Delete submenu.

Traffic Managtement Service	*Capabilities Verification*	*Performance Criteria*
	Delete provides for the removal of an existing Reroute.	Click on the Test reroute Click on OK. A confirmation window appears. Click on OK to confirm the deletion..
Tools	Send Send is used to send displayed reroutes from any TSD in the system to all other TSDs in the system. The principle user is the ATCSCC,	